

Xpeed 320R

SDSL Router



User's Guide

Xpeed 320R

SDSL Router

COPYRIGHT

All rights reserved. Reproduction, adaptation, or translation of any part of this document without prior written permission from Xpeed, Inc. is prohibited, except as allowed under copyright laws.

(C) Copyright 2000 - Xpeed Networks, Inc.

STATEMENT OF CONDITIONS

In the interest of improving product functionality and/or reliability, Xpeed Networks, Inc. reserves the right to make any changes to the products described in this document without notice.

TRADEMARK

Xpeed and the Xpeed logo are registered trademarks of Xpeed Networks, Inc.

All other brand and product names are registered trademarks of their respective holders.

FCC COMPLIANCE STATEMENT

This equipment has been tested and bound to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation. This equipment generates, uses, and can radiate radio frequency energy. If this equipment is not installed or used in accordance with the instructions, it may cause harmful interference to radio communications.

CONTACT

Xpeed Networks, Inc.
99 West Tasman Drive, Suite 110
San Jose, CA 95134

Main: 408-473-8804
Fax: 408-473-8808

www.xpeed.com
info@xpeed.com

PART NUMBER

XP400-0019

Revision 1.0

Table of Contents

Introduction	9
What is SDSL?	9
The X320R	10
Major Features	10
Physical Description	11
Speeds Supported	13
Router Configuration and Management	13
Before You Begin	15
Box Contents	15
Internet Service Information	16
Additional Requirements	17
Setting up the X320R	19
Hardware Setup	19
Xspeed Quick Start	21
System Requirements	21
Product Information Window	22
LAN Configuration Window	23
WAN Configuration Window	24
PPP Configuration Window	25
DSL Configuration Window	26
RIP2 Configuration Window	27
Update Window	28
Advanced Window	29
Xspeed Web Interface	31
Getting Started	31
Product Information Window	33
Interface Configuration Window	34
IP-Filter Configuration Window	38
NAT Map Configuration Window	40
NAT Redirect Configuration Window	41
DHCP Subnet Configuration Window	42

Route Table Configuration Window	43
Password Window	43
Download Firmware Window	44
Reboot Window	44
Xpeed Command Line Interface	45
RS232 Serial Interface	45
Telnet Session	48
CLI Commands	51
Add	51
Alias	55
Delete	56
Disable	57
Enable	57
Exit	58
Help	58
Logout	59
Modify	59
Password	62
Ping	63
Quit	63
Reboot	63
Restore	64
Save	64
Show	64
TFTP	67
Traceroute	67
Unalias	68
IP Networking Basics	69
What is a Router?	69
IP Addressing	70
Netmask	71
Subnet	71
Network Address Translation	72
LAN Address Assignment	73
Miscellaneous	74

More Info	74
Sample Application	75
Small Office Profile	75
DHCP	76
How to Set It Up	77
To Add More Users	80
Trouble Shooting	81
Frequently Asked Questions	85
Default Settings	89
Technical Specifications	93
Glossary	97

Chapter 1

Introduction

Congratulations on your purchase of the Xpeed 320R SDSL to Ethernet Router.

The 320R enables you to share with other users on the Local Area Network (LAN) a high-speed SDSL line that may be intended for a single user.

This user's guide will help you understand the features of your 320R and guide you in the installation and configuration.

1. WHAT IS SDSL?

SDSL is an acronym for Symmetrical Digital Subscriber Line, which is a technology that improves the amount of information that can be transmitted on existing copper phone lines. With SDSL, users can connect to the Internet at speeds up to 2.3 Mbps, which is about 50 times faster than a connection over a 56K analog modem.

SDSL is symmetric, because both upstream and downstream speeds are the same. This differs from Asymmetric Digital Subscriber Line (ADSL) which usually has a higher downstream rate than upstream rate. ADSL is best suited for applications such as multimedia, where the user is mostly receiving large volumes of information but transmitting only a small amount of information. SDSL, on the other

hand, is symmetric so users can send and receive at equally high rates. This allows applications such as email server, web server, and video conferencing.

2. THE X320R

The Xpeed X320R is an integrated SDSL to Ethernet IP router providing high-speed WAN connectivity for home offices and small businesses. The X320R is based on SDSL technology, providing businesses a reliable symmetric connection critical for day to day operation. In addition, the X320R is an IP router supporting features such as Network Address Translation (NAT) and firewall that are part of the core of a business connection.



3. MAJOR FEATURES

The X320R is a DSL access device for high speed connectivity. It is built to provide users with several business class features, focusing on the most important ones. Some of the major features of the X320R are listed below.

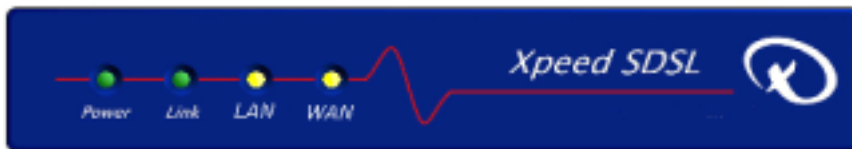
- Up to 2.3 Mbps speed
- Frame Relay
- Integrated four port hub
- NAT/PAT

- RIP1/RIP2
- DHCP server and client
- Quick Start application
- Web based interface
- Remote management
- Scripting
- One touch firmware upgrades
- Firewall
- PAP/CHAP

4. PHYSICAL DESCRIPTION

The X320R comes in a sturdy compact chassis that can be stacked or wall mounted. It should be placed as close as possible to the DSL jack to reduce noise and interference. PCs may be connected directly to the X320R or through Ethernet hubs.

- Width: 7 3/4 in (20 cm)
- Depth: 5 1/8 in (13.5 cm)
- Height: 1 1/8 in (3 cm)
- Holes for wall mounting: 3 15/16" (10 cm) center to center

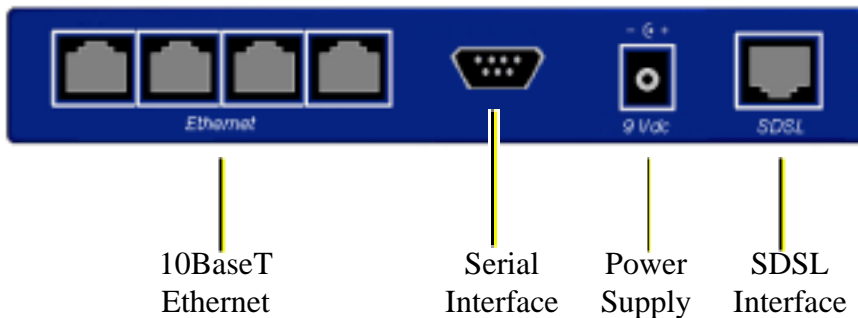


The X320R has four LEDs on the front to indicate system status.

LED	Description
Power	Power is on or off

LED	Description
Link	DSL connection established
WAN	Data activity on DSL port
LAN	Data activity on Ethernet port

If your modem is not functioning properly, please refer to the Trouble Shooting section in the Appendix for detailed directions on using the LEDs to help locate your problem.



The X320R has the following ports on the back:

10BaseT Ethernet interface is the connection to the LAN. The four ports function as a built-in hub, allowing up to 4 PCs to be connected directly to the X320R. Additional PCs may be added by connecting one or more of the ports to an external hub. Please refer to the Network Planning section for more information. This interface does not support 100BaseT.

Each Ethernet port has a set of LEDs to indicate link status and data activity. The green top left LED is lit when an Ethernet connection is established with another device, either an Ethernet adapter in a PC or an external Ethernet hub. The yellow LED at top right flashes to indicate data activity on that port.

Serial Interface is used to manage and configure the X320R through a RS232-based terminal application.

Note: On versions of the X320R that have a metal chassis, the connector is a male DB9. On plastic versions, the connector is a female DB9.

Power Supply is connected to the enclosed 9 VDC wall transformer. Use only the wall transformer supplied with your product.

SDSL Interface is the port that connects to the SDSL line provided by your ISP.

5. SPEEDS SUPPORTED

The X320R supports an SDSL interface to the WAN. This allows the X320R to connect at speeds up to 2.3 Mbps in either transmit or receive directions. However, the actual speed that the X320R will operate will depend upon the type of service that you selected through your ISP. If you find that you need a faster connection, please contact your ISP to discuss the options available to you.

6. ROUTER CONFIGURATION AND MANAGEMENT

The X320R may be configured by four methods: Quick Start, web browser, serial port terminal emulation, and remote TELNET session. The Quick Start and web browser interfaces are graphical and intended for getting users started fast. The serial port and TELNET interfaces are based on the powerful Command Line Interface (CLI) and is intended for advanced users.

Chapter 2

Before You Begin

Before proceeding with the installation and setup of your new X320R, please read through the following sections to verify that you have everything that you will need.

1. BOX CONTENTS

Please verify that you have each of the items listed below. If you are missing any item, please contact Customer Service.

- X320R SDSL to Ethernet Router.
- X320R User's Guide (on CD)
- X320R installation software.
- X320R Quick Start Guide
- A power adapter.
- A RJ11 SDSL cable
- A straight-thru Category 5 Ethernet cable.

2. INTERNET SERVICE INFORMATION

Please contact your Internet Service Provider (ISP) to complete the table below. You may complete the table below, or use the guide provide on the Quick Start sheet. This information will be used to complete the configuration of your router.

If you are installing your X320R yourself, you may need the following information about your SDSL account from your ISP:

- This account must support routing.
- Is your service auto-detect for speed? _____
- If not, what speed is your service set at? _____
- What framing type is to be used across the SDSL link? _____
- Is LMI to be used on the SDSL link? _____
- What SwitchType is used on the SDSL link? _____

If IP Address is static, the following information is required:

- What is your IP Address? _____ . _____ . _____ . _____
- What is your Subnet Mask? _____ . _____ . _____ . _____
- What is your Gateway Address? _____ . _____ . _____ . _____
- What is your Primary DNS Addresses? _____ . _____ . _____ . _____
- What is your Secondary DNS Addresses? _____ . _____ . _____ . _____

If you have a PPP connection, the following information is required:

- What type of Authentication is being used? _____
- What Chap type is being used? _____
- Is IP header compression being used? _____
- What is your User ID? _____
- What is your Password? _____

3. ADDITIONAL REQUIREMENTS

The X320R is best suited for use in a multi-user Ethernet based LAN environment. The LAN layout should be a network of PCs interconnected by Category 5 Ethernet cables.

Each PC must be able to communicate with the network. The PC may use an Ethernet Network Interface Card (NIC) or some other form of Ethernet adapter. In addition, the PC must be setup with TCP/IP.

If you want to connect an external hub to the X320R, you may require a cross-over Ethernet cable. However, you can use a standard Category 5 straight-thru cable if the hub has an **Uplink** switch to implement the cross-over functionality.

You may also need a DB9 Serial Cable to configure the X320R via the serial port. However, if you do not have a serial cable, you can use any of the other methods to manage the X320R including TELNET, web interface, and Quick Start.

Chapter 3

Setting up the X320R

Once you have all the information that you will need, you can follow the steps below to begin the installation and setup of the X320R.

1. HARDWARE SETUP

1. Locate a secure spot for your X320R router so people do not trip over it loosening any cables. It should be located as close as possible to the DSL jack to reduce possible interference. Note: you may use the holes on the bottom of the X320R to mount it on a wall.
2. Plug the wall transformer to a 110 VAC socket. Then power the X320R by connecting the wall transformer to the 9VDC jack on the back of the X320R. You should immediately see the power LED turn on.
3. Connect the SDSL Line to the DSL port on the back of the X320R. You should see the Link LED start to blink and eventually light solid green. If this LED does not turn solid after 5 minutes, please check to make sure your connectors are properly seated.

4. Connect the X320R to your LAN. If you have less than four PCs in your network, you can connect them directly into the integrated 4-port hub on the X302R. However, if you have more than 4 PCs, you will have to use one of the ports for an external Ethernet hub.

Chapter 4

Xpeed Quick Start

Quick Start will help you view and modify the configuration of your X320R router. Quick Start is a Windows-based application, and will run only on Windows OSes. If you want to use a Macintosh or UNIX based system to manage the X320R, please use the HTML based interface that can be accessed from any system supporting a web browser such as MS Internet Explorer or Netscape Navigator.

1. SYSTEM REQUIREMENTS

To use Quick Start, you will need to have one of the following operating systems:

- Windows 95
- Windows 98
- Windows NT 4.0
- Windows 2000

For Windows 95, you need to have Winsock 2 installed. Please refer to the FAQ for information on locating installation files for Winsock.

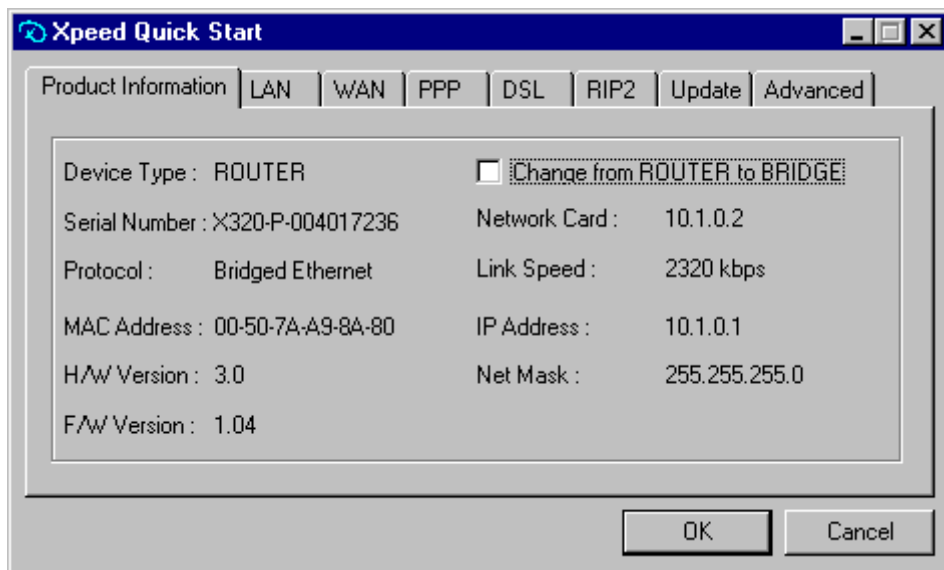
The installation software for Quick Start is located on your distribution CD under the QuickStart directory. Once you have located this directory, simply run the **setup.exe** file to install Quick Start.

When you start Quick Start, it will automatically connect to the X320R over the LAN Ethernet. If it is unable to detect the X320R, please check that your cables are connected properly.

The Quick Start window is organized by functionality. You can select the information being displayed via the tab buttons across the top of the window. Simply click on the desired subject to access information in that area.

Note: You will not be asked to log into the system until you try to make any modifications.

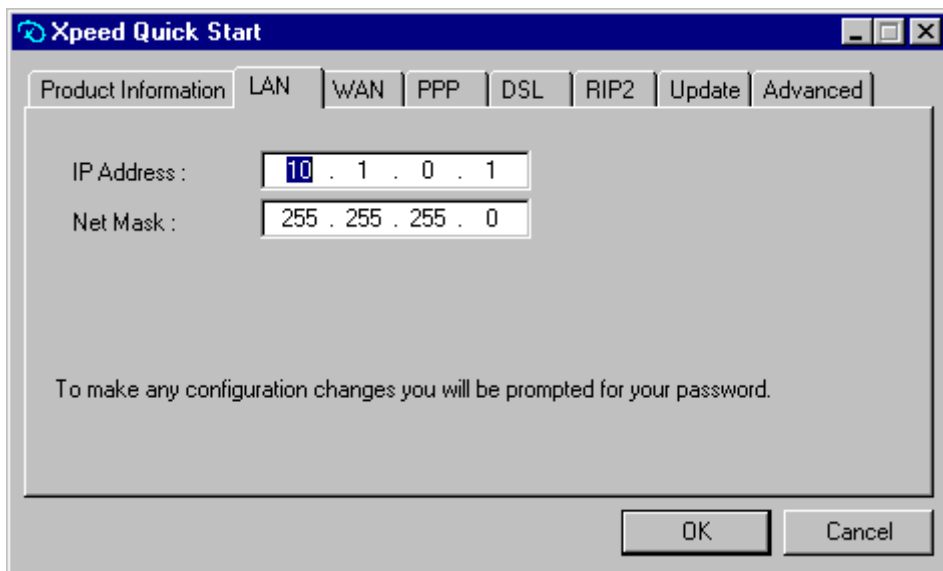
2. PRODUCT INFORMATION WINDOW



This page displays general information about your unit including manufacturing information, version, and line configuration.

Select **Change from ROUTER to BRIDGE** to disable the Router mode and operate only as a Bridge.

3. LAN CONFIGURATION WINDOW



The image shows a screenshot of the 'Xpeed Quick Start' LAN Configuration window. The window has a title bar with the text 'Xpeed Quick Start' and standard window controls. Below the title bar is a tabbed interface with tabs for 'Product Information', 'LAN', 'WAN', 'PPP', 'DSL', 'RIP2', 'Update', and 'Advanced'. The 'LAN' tab is currently selected. In the main area of the window, there are two input fields: 'IP Address' and 'Net Mask'. The 'IP Address' field contains the value '10 . 1 . 0 . 1' and the 'Net Mask' field contains '255 . 255 . 255 . 0'. Below these fields, there is a text box containing the message: 'To make any configuration changes you will be prompted for your password.' At the bottom right of the window, there are two buttons: 'OK' and 'Cancel'.

This page allows you to modify your LAN settings.

IP Address - This is the IP Address of your X320R. It is what the PCs on your LAN will see as their gateway.

Net Mask - Net Mask of your network

4. WAN CONFIGURATION WINDOW

Xpeed Quick Start

Product Information | LAN | **WAN** | PPP | DSL | RIP2 | Update | Advanced

IP Address : 0 . 0 . 0 . 0 DLCI : 16

Net Mask : 0 . 0 . 0 . 0 Frame Type : Bridged Ethernet

Default Gateway : 172 . 23 . 7 . 177

☒ Obtain an IP address from a DHCP server

To make any configuration changes you will be prompted for your password.

OK Cancel

This page allows you to view and modify your WAN configurations for TCP/IP and Frame Relay.

IP Address - This is the IP address assigned to you by your ISP.

Net Mask - This is the Net Mask assigned to you by your ISP.

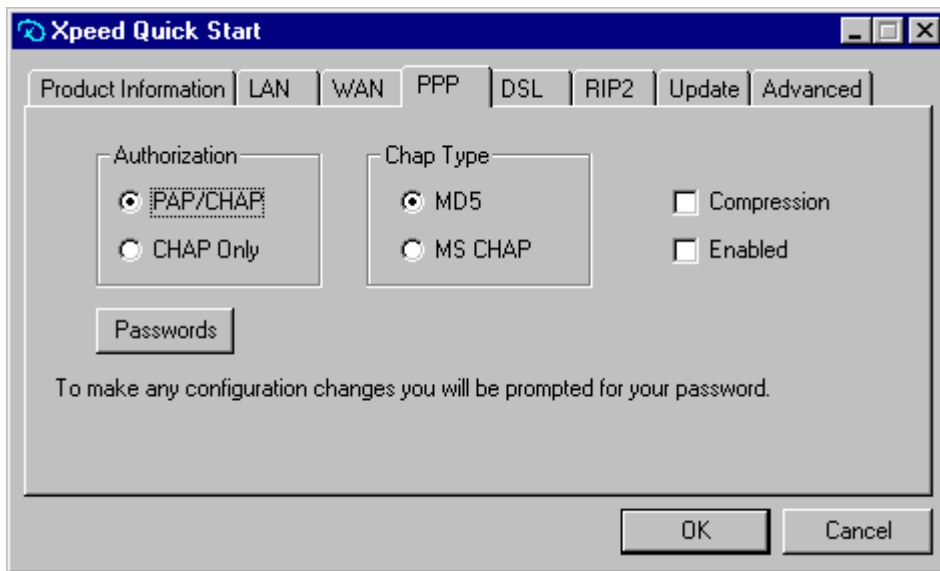
Default Gateway - This is the Gateway address assigned to you by your ISP.

Obtain an IP address from a DHCP server - This allows the X320R to function as a DHCP client, thus receiving a dynamic IP address from the provider's DHCP server.

DLCI: This displays the current DLCI value.

Frame Type: This allows you to select or modify your WAN protocol. Please check with your ISP for the correct setting.

5. PPP CONFIGURATION WINDOW



This page allows you to view and modify PPP configurations. Note: this section is necessary only if your WAN connection is based on PPP and not Frame Relay.

Authorization -

PAP/CHAP allows negotiation between PAP and CHAP

CHAP Only does not allow for negotiation

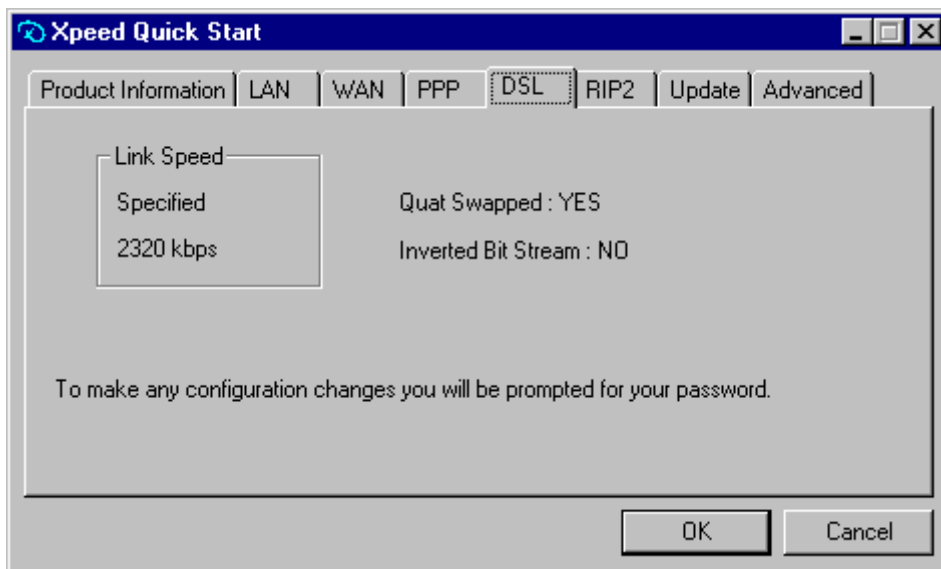
CHAP Type - If using CHAP, select between MD5 and Microsoft CHAP.

Compression - Select to enable header compression.

Enabled - Select to enable PPP otherwise defaults to Frame Relay.

Passwords - Modify user ID and password for PPP account.

6. DSL CONFIGURATION WINDOW



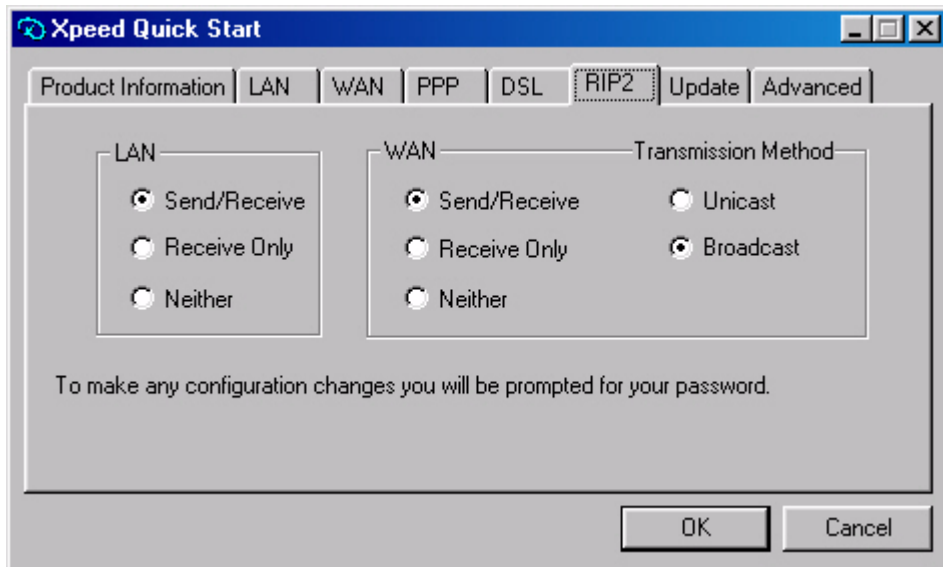
This page allows you to make view your DSL line settings. No modifications can be made to this page.

Link Speed - The link speed assigned to you by your ISP.

Quat Swapped - Displays the status of Quat Swap.

Inverted Bit Stream - Displays status of the Inverted Bit.

7. RIP2 CONFIGURATION WINDOW



This page allows you to configure RIP2 for your router.

WAN - Select how to handle RIP2 information:

Send and Receive

Receive Only - Receive but not send

Neither - ignore RIP2 information

Transmission Method - allows the transmission of RIP information via a normal broadcast address or via a unicast address

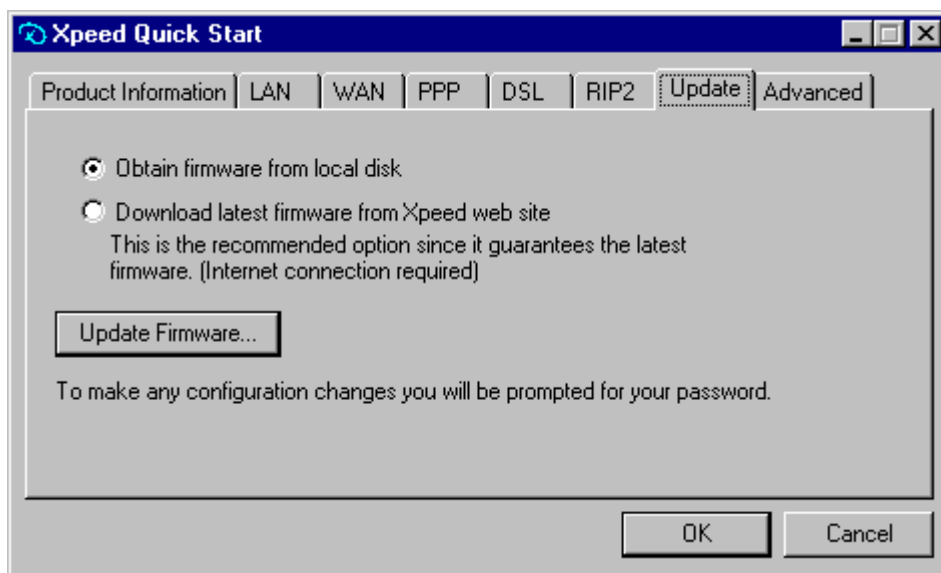
LAN - Select how to handle RIP2 information:

Send and Receive

Receive Only - Receive but not send

Neither - ignore RIP2 information

8. UPDATE WINDOW

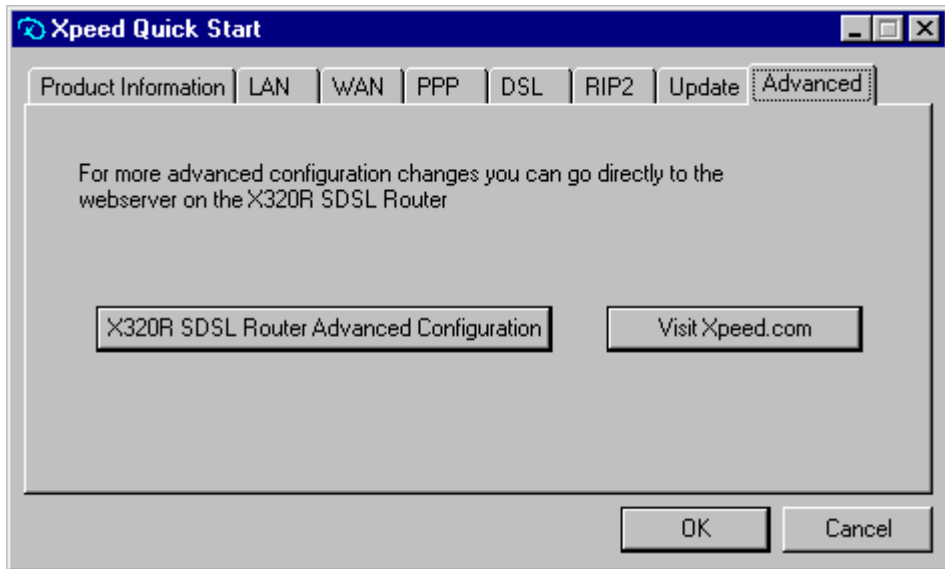


This page will help you update the firmware on your X320R. Note: It is possible that an upgrade may effect your current configuration.

Obtain firmware from local disk - Select this option if the target firmware that you want to upgrade to is located on the hard drive of your PC. This does not require a DSL connection. If you are having firmware trouble with your connection, you will have to use this option.

Download latest firmware from Xpeed web site - This will automatically retrieve the firmware from the Xpeed server. This allows you to upgrade to the latest version of the firmware. However, you must have a working DSL connection.

9. ADVANCED WINDOW



X320R SDSL Router Advanced Configuration - This directs you to the X320R Web Interface to modify advanced features.

Visit Xpeed.com - This directs you to the Xpeed web site. A connection must be pre-established.

Chapter 5

Xpeed Web Interface

The web interface is a graphical and flexible method to fully access the X320R for configuration and maintenance. Because it is based on HTML, it can be used from any type of operating system including Macintosh, UNIX, and Linux. Simply launch any web browser such as Internet Explorer or Netscape Navigator.

1. GETTING STARTED

To access the X320R using the web interface, open a web browser and enter the IP Address of your router in the address bar. The default address for the X320R is 192.168.1.1.



Note: You must access the X320R using a web browser from a PC that is located on the same subnet as the X320R. If the X320R is on a different subnet from your PC, you must change one of their addresses to make both address coexist with the same subnet.

The browser will establish a connection to the X320R which will prompt you for a user name and password.

There are two different accounts available:

- system - allows administrative control over the X320R
- guest - allows the user to only view X320R settings



Please type **system** to login under the administrative account. Then type in your password (default is `system`). If you are successful, the X320R will display the Interface Configuration page in your browser.

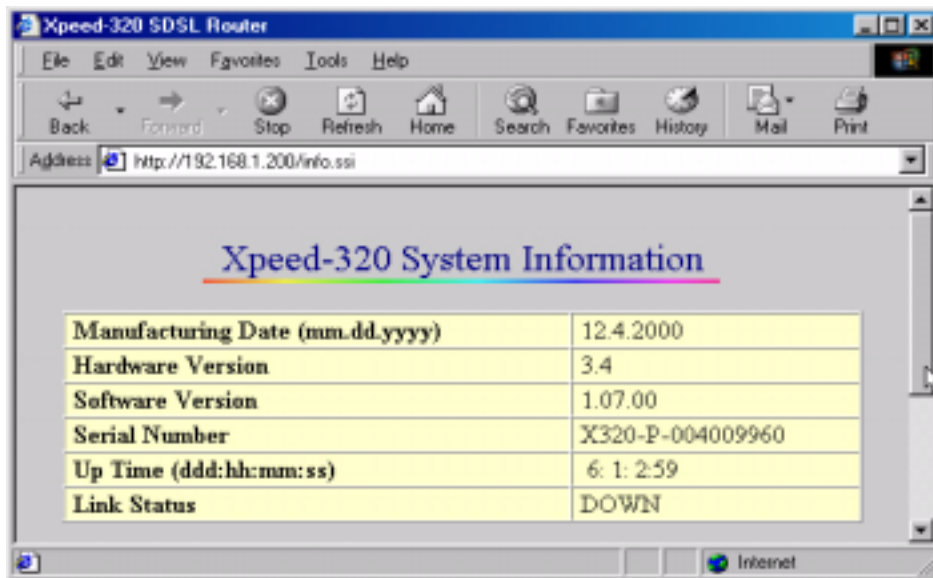
The X320R Web Interface has several different pages to help organize the configurations by functionality. The following sections describe each page in more detail.

MAKING CHANGES

To make any changes to any of the X320R configurations, please follow these steps:

- Select the modify box at the left of the subject
- Make the desired changes
- Click on the APPLY button at the bottom of the page

2. PRODUCT INFORMATION WINDOW



This page displays system information regarding the X320R:

Manufacturing Date is the date on which your X320R unit was completed.

Software Version is the firmware version installed within the X320R.

Hardware Version is the version of the X320R hardware.

Software Version is the version of the software running on your X320R.

Serial Number is your serial number

Up Time is the duration that your X320R has been running since booting. Format is *day:hour:minute:second*.

Link Status tells the status of the WAN link

3. INTERFACE CONFIGURATION WINDOW

This is the default page that comes up when you initially access the X320R using the Web Interface. This page allows you to configure any of your interfaces and connection protocols.

LAN CONFIGURATION

LAN Configuration				
Modify	Interface ID	IP Address	Net Mask	DHCP Server
<input type="checkbox"/>	L0	192.168.1.200	255.255.255.0	<input type="checkbox"/>

Only one LAN interface may exist, L0.

IP Address - allows you to modify the IP address of the X320R.

Net Mask - is the net mask for the LAN.

DHCP Server - allows the X320R to provide dynamic IP addresses to PCs on the LAN (PCs must also be configured with DHCP).

WAN CONFIGURATION

Modify	Add	Delete	Interface ID	IP Address	Net Mask	Gateway	DLCI	Framing Type	DHCP Client Enabled
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	w0.0	0.0.0.0	0.0.0.0	0.0.0.0	16	RFC1483 MAC ENCAPS	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	w0.1					RFC1483 IP Routing	<input type="checkbox"/>

It is possible to have multiple WAN interfaces if your ISP provides you with multiple connections. You may Add, Delete or Modify WAN interfaces using the buttons. Be sure to click APPLY to execute your changes. Note: if using PPP there can only be one WAN interface due to the nature of PPP

Interface ID - when adding a new interface, you must select an Interface ID.

IP Address - is the IP address assigned to you by your ISP if assigned statically. If using DHCP client you would put 0.0.0.0 as the IP address.

Net Mask - is the subnet mask. If using DHCP client you would put 0.0.0.0 as the NetMask

Gateway - is the address of your ISP gateway. If using DHCP client you would put 0.0.0.0 as the gateway

DLCI - The default interface w0.0 is set at 16.

Framing Type - allows you to select the type of connection that you have. Please contact your ISP for this information.

DHCP Client allows your X320R to receive an IP address dynamically from the ISP.

Enabled allows you to have a configured interface but have it either enabled or disabled.

FRAME RELAY CONFIGURATION

Frame Relay Configuration				
Modify	Port ID	Termination	Switch Type	LMI
<input type="checkbox"/>	W0	<input type="radio"/> Line Termination <input checked="" type="radio"/> Network Termination	<input checked="" type="radio"/> ANSI <input type="radio"/> Q.933	<input type="radio"/> On <input checked="" type="radio"/> Off

This entry allows you to make modifications to the configuration of the Frame Relay connection.

Termination - the X320R can operate in two modes:

- Line Termination (LT) - This mode will allow you to use the X320R in a back-to-back mode. A device in LT mode will emulate signaling coming from a DSLAM.
- Network Termination (NT) - This is the default operating mode of the X320R.

Switch Type - This setting allows you to select the switch type. This is typically set to ANSI for North America. Q.933 is the typical switch type in Europe

LMI - allows you to enable Local Management Interface

PPP CONFIGURATION

PPP Configuration								
Modify	Port ID	Authentication	Chap Type	IP Header Compression	Enabled	User ID	Password	Re-Enter Password
<input type="checkbox"/>	W0	<input checked="" type="radio"/> Auto <input type="radio"/> Chap Only	<input checked="" type="radio"/> MD5 <input type="radio"/> MS CHAP	<input type="radio"/> Compressed <input checked="" type="radio"/> Not Compressed	<input type="radio"/> Enabled <input checked="" type="radio"/> Not Enabled	<input type="text"/>	<input type="text"/>	<input type="text"/>

This entry allows you to make modifications to the configuration of the PPP connection.

Port ID - Allows the user to select which WAN interface to configure PPP

Authentication - select between automatic authentication or Challenge Handshake Authentication Protocol.

CHAP Type - select between MD5 and Microsoft CHAP.

IP Header Compression - Enable or disable compression.

Enabled - Allows the user to enable/disable PPP on the particular WAN interface

User ID - User Name associated with PPP account.

Password - Password associated with PPP account.

RIP2 CONFIGURATION

RIP2 Configuration			
Modify	LAN	WAN	WAN Transmission Method
<input type="checkbox"/>	<input checked="" type="radio"/> Send/Recieve <input type="radio"/> Receive Only <input type="radio"/> Neither	<input checked="" type="radio"/> Send/Recieve <input type="radio"/> Receive Only <input type="radio"/> Neither	<input type="radio"/> Unicast <input checked="" type="radio"/> Broadcast

LAN - enables RIP2 protocol on the LAN interface. The X320R can either be set to send/receive routing updates, receive only, or disable RIP2 on the LAN interface. Routing update packets from routers running RIP1 is also supported by the X320R.

WAN - enables RIP2 protocol on the WAN interface. The X320R can either be set to send/receive routing updates, receive only, or disable RIP2 on the WAN interface. Routing update packets from routers running RIP1 is also supported by the X320R.

WAN Transmission Method - On the WAN interfaces 2 types of RIP2 routing updates are supported for transmission across the WAN link. These 2 types are unicast, ie. directed update packets, and broadcast, ie. sent to all devices on the network.

DSL CONFIGURATION**DSL Configuration**

Modify	Port ID	Quat Swapped	Inverted Bit Stream	Link Speed
<input type="checkbox"/>	W0	<input checked="" type="radio"/> No <input type="radio"/> Yes	<input checked="" type="radio"/> No <input type="radio"/> Yes	AUTO

This entry allows you to configure parameters related to the DSL line.

Quat Swapped - Set to **No** unless specified otherwise by your ISP.

Inverted Bit Stream - Set to **No** unless specified otherwise by your ISP.

Link Speed - Please check with your ISP for the speed assigned to your service. If your ISP supports autodetect, you may select that option.

4. IP-FILTER CONFIGURATION WINDOW

Delete	Rule #	Rule
<input type="checkbox"/>	1.1	block 1 block in quick proto tcpip from any to any port = 135 to 138
<input type="checkbox"/>	1.2	group 1 block in quick proto TCP from any to any port = 2049
<input type="checkbox"/>	1.3	group 1 block in quick proto TCP from any to any port = 111
<input type="checkbox"/>	1.4	group 1 block in quick proto TCP from any to any port = 108
<input type="checkbox"/>	1.5	group 1 block in quick proto TCP from any to any port = 114
<input type="checkbox"/>	1.6	group 1 block in quick proto TCP from any to any port = 143
<input type="checkbox"/>	1.7	group 1 block in quick from any to any with short flag
<input type="checkbox"/>	2.1	block 2 block in quick proto tcpip from any port 127 to 129 to any
<input type="checkbox"/>	2.2	group 2 block in quick proto UDP from any port = 2049 to any
<input type="checkbox"/>	2.3	group 2 block in quick proto UDP from any port = 111 to any
<input type="checkbox"/>	2.4	group 2 block in quick from any to any with short flag

This page allows you to add and delete IP filter rules. Filter rules are executed in the order in which they are listed, where 1 is the first rule, so it is important to keep track of their respective order.

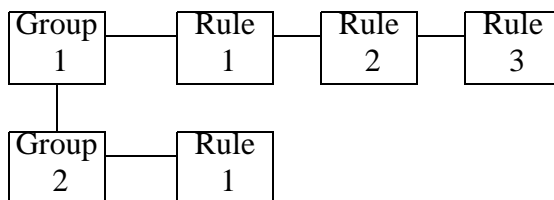
This is the page that is displayed when you add a filter rule

Group # - Specify the Group order number.

Rule # - Specify the Rule order number.

[illegible]

Rules belong to a group of rules. When the quick option is used for the head rule and the first rule in a group is not satisfied, none of the other rules in that group will be evaluated. If the quick option is not used the other rules in the group will be processed normally therefore all of the rules in that group must be evaluated before proceeding to the next group of rules. This can cause a degradation in performance due to processing rules that should not be processed. In the diagram below both head rules 1.1 and 2.1 are being used with the quick option enabled, Group #1 Rule #1 must be satisfied for Group #1 Rule #2 to occur. If group #1 Rule #1 is not a match the filtering process skips over the rest of Group #1 rules and starts directly evaluating Group #2 Rule #1. There are 8 groups with 8 rules each.



For instance, if a user created 2 groups of rules, Group #1 rules for traffic coming in the LAN interface and Group #2 rules for traffic coming in the WAN interface. If a packet came in the WAN interface you would want the filtering process to skip over any LAN rules and start evaluating the WAN rules. This would be accomplished by specifying a head rule of 1.1 with quick enabled and specifying any traffic coming in the LAN interface and creating a head rule of 2.1 with quick enabled and specifying any traffic coming into the WAN interface. You would then create any other rules for Group #1 to be dedicated to processing traffic coming into the LAN interface and would create any other rules for Group #2 to be dedicated to processing traffic coming into the WAN interface. If quick were not enabled for head rule 1.1 the router would process all of Group #1 rules before proceeding to Group #2 which are the incoming WAN rules.

Action - Specify filter action: traffic pass through or traffic blocked by X320R

- **Pass** - When a filter matches the rule, pass allows the traffic to be allowed through the X320R.
- **Block** - When a filter matches the rule, the traffic is not allowed through the X320R.

Return-ICMP (Host-Unr) - When rule is matched and traffic is blocked this setting returns an ICMP host unreachable packet to the originating host.

Return-ICMP (Need-Frag) - When rule is matched and traffic is blocked this setting returns an ICMP fragmentation needed and DF set packet to the originating host.

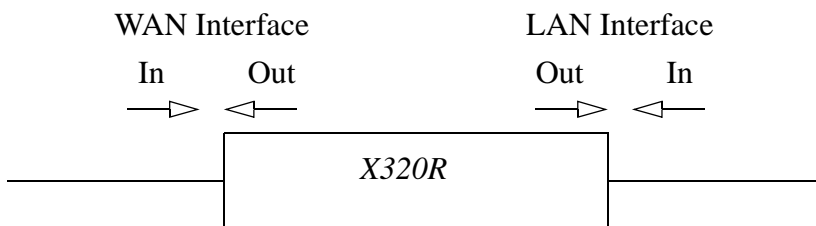
Return-ICMP (Net-Unr) - When rule is matched and traffic is blocked this setting returns an ICMP Network unreachable packet to the originating host.

Return-ICMP (Port-Unr) - When rule is matched and traffic is blocked this setting returns an ICMP Port unreachable packet to the originating host.

Return-ICMP (Proto-Unr) - When rule is matched and traffic is blocked this setting returns an ICMP Protocol unreachable packet to the originating host

Return-ICMP (SRCFAIL) - When rule is matched and traffic is blocked this setting returns an ICMP Source Route Failure packet to the originating host

In/Out - Location of filter with respect to interface. **In** refers to the direction going “in” to the X320R. **Out** refers to direction going “out” of the X320R.



Quick - The importance of rule order is that the X320R will execute the last instance of common or conflicting rules. Quick forces the first matching rule to be executed first and then exit the filtering process before processing any of the other matching rules. The only exception to this is if the rule that has quick enabled is a head rule, in this case if the rule is matched the rest of the rules in the group are processed otherwise the rest of the rules in the group are skipped and the filtering process starts evaluating the next group of rules.

Interface ID- Selects the interface that the rule is applied to.

- **TOS-** When using this parameter traffic is filtered based on Type of Service. Typically this option is not used.
- **TTL-** When using this parameter traffic is filtered based on the Time to Live portion of the packet. This value must exactly match the TTL of the packet. Typically this option is not used.

Interface ID- Selects the interface that the rule is applied to.

- **Duplicate To-** causes the packet to be copied, and the duplicate packet to be sent outbound on the specified interface, optionally with the destination IP address changed to that specified. This is useful for off-host logging, using a network sniffer. Consider a case where it is required to monitor all tcp connections for some traffic analysis. In such a case the packet could be directed to a particular host where a program would be listening on a specific interface and would then analyze the packet. This option is not typically used for most applications.

TTL-

Protocol - This specifies whether you would like to specifies the protocol type you would like the filter to process.

- **NONE** - Specifies that the filter to ignore the layer 4 information in the packet.
- **TCP/UDP** - Specifies the filter only apply to TCP or UDP packets.
- **TCP** - Specifies that the filter only apply to TCP packets.
 - TCP Flags** - Although not normally used, the filtering process also supports filtering on the TCP flags. This is effective for TCP filtering. Each letter indicates the possible flags that could be checked against in the packet. The various flags could be used in combination. Thus SA would represent a SYN-ACK combination. It is also possible to set a mask indicating which TCP flags the user wishes to compare to. This would be mainly to guard against weird aberrations. The mask flags indicate which bits of the TCP flags the user is interested in checking. When using the SYN bit in a check, the user should specify a mask to

ensure that the filter cannot be defeated by a packet with SYN and URG flags. Thus, the flags SA becomes SA with AUPRFS mask flags which match any packet with ONLY the SYN and ACK flags set.

The available TCP flags available are listed below:

F - FIN

S - SYN

R - RST

P - PUSH

A - ACK

U - URG

- UDP - Specifies that the filter only apply to UDP packets.
- ICMP - Specifies that the filter only apply to ICMP packets.

- ICMP Options - This allows the user to filter on ICMP message types.

The types of messages that can be filter on are listed below.

echo - Echo

echorep - Echo Reply

inforesp - Information Reply

inforeq - Information Request

maskrep - Mask Reply

maskreq - Mask Request

paramprob - Parameter Problem

redir - Redirect

squench - Source Quench

timest - Timestamp

timestrep - Timestamp Reply

timex - Time Exceeded

unreach - Destination Unreachable

(0-255)

Value Dec#

(0-255)

Source - Specifies the source of traffic to block or allow.

- Any - Specifies traffic from any IP address. This is normally used in conjunction with a specific destination address or port.
- Specific - Specifies the filter to block or allow a specific source IP with specific netmask

Source Port - Specifies a source port # or range of source port #s the filtering process attempts to match against

- No Comparison - Specifies the filtering process to ignore the source port of packets for the specific filter
- Comparison - Here the user can compare against a specific source port or range of source ports. The suboptions for comparison are given below
 - EQ - Specifies the filter to match against the specific port or range of ports.

NE - Specifies the filter to match against all ports not equal to the specific port or range of ports.

LT - Specifies the filter to match against all ports less than the specific port or range of ports.

LE - Specifies the filter to match against all ports less than or equal too the specific port or range of ports

GT - Specifies the filter to match against all ports greater than the specific port or range of ports.

GE - Specifies the filter to match against all ports equal to or greater than the specific port or range of ports.

Destination - Specifies the destination of traffic to block or allow.

- Any - Specifies traffic going to any IP address. This is normally used in conjunction with a specific source address or destination port.
- Specific - Specifies the filter to block or allow a specific destination IP & netmask

Destination Port - Specifies a specific destination port # or range of port #s the filtering process attempts to match against

- No Comparison - Specifies the filtering process to ignore the destination port of packets for the specific filter
- Comparison - Here the user can compare against a specific destination port or range of destination ports. The suboptions for comparison are given below

EQ - Specifies the filter to match against the specific port or range of ports.

NE - Specifies the filter to match against all ports not equal to the specific port or range of ports.

LT - Specifies the filter to match against all ports less than the specific port or range of ports.

LE - Specifies the filter to match against all ports less than or equal too the specific port or range of ports

GT - Specifies the filter to match against all ports greater than the specific port or range of ports.

GE - Specifies the filter to match against all ports equal to or greater than the specific port or range of ports.

For example, a user may wish to block traffic coming from any LAN IP source address going to the internet and surfing the web. For this example the user would create a filter *blocking* any *LAN* address going *Out* the WAN interface going *TCP port equal to 80*.

With Options - Although, not normally used in most applications the with options allow one to allow various combinations.

- None - the default
- With
 - Not - Matches when only the negative of the following options are used.
 - Short - means that there is a match if the packet is short.
 - Frag - means that there is a match if the packet is fragmented.
- And - allows multiple filter matches. For instance if the user wanted to match on short and fragmented packets they would use this option.

Keep Options - The keep options can only be used when the protocol is TCP, UDP, or TCP/UDP.

- None - No keep options are enabled, the default
- State - This option which is normally used in conjunction with outgoing rules, allows response packets back into the router that originated within the router. For instance, if the user wanted to create a filter to block all packets coming into a router from the WAN side and was using traditional routing and not NAT between the interfaces. The user could create the first rule to allow any TCP/UDP packets out of the WAN interface with Keep State enabled. Then the user could create a second rule to block all incoming packets to the WAN interface. What this does is when a TCP/UDP packet is initiated through the LAN interface through the WAN interface a state entry is made in a state table within the router. When a response comes back to the WAN interface the packet state information is checked against the state table within the router, if there is a match the packet is allowed back onto the LAN side. Otherwise, if the keep state was not enabled, when the response would come back to the WAN side of the router the packet would be dropped.
- Frags - This option allows packets that would otherwise not match a filter, due to fragmentation, to match the filter if the packets are fragmented. For instance if there was a filter that allowed packets destined

to port 90 allowed in the router, if any of these packets were fragmented they would not be allowed in the router unless this option was enabled.

5. NAT MAP CONFIGURATION WINDOW

Delete	Add	Interface ID	Source	
			IP	Mask
<input type="checkbox"/>	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

Destination		Protocol	Port Range	
IP	Mask		From	To
<input type="text"/>	<input type="text"/>	tcp	<input type="text"/>	<input type="text"/>

This page allows you to add and delete NAT rules. One of the key features of NAT is the ability to map multiple IP addresses on your LAN to a single IP address going out to your ISP.

Interface ID - Specify the interface across which the mapping occurs, typically the WAN interface. Default WAN interface would be w0.0

Source - Source of mapped traffic. This is typically the address(s) that are your local LAN stations that want to access the Internet or Corporate network. You can use individual PC addresses as a source with corresponding host specific masks, ie. 255.255.255.255 or you can use a network address with network specified masks, normally 255.255.255.0. If you are using the X320R default LAN network address of 192.168.1.0 this would be your source and the mask would be 255.255.255.0.

Destination - Destination of mapped traffic. For example, if your ISP provided you with a WAN IP address of 209.141.176.154, that is your destination address. You would then specify a host specific mask of 255.255.255.255 since you are doing the mapping to 1 specific WAN IP address.

Protocol - Transport protocol. Typically TCP/UDP. Normally 2 NAT rules must be created. One using the protocol of TCP/UDP and one using no protocol or port numbers. This is so ICMP traffic can traverse the router since ICMP traffic does not use port numbers.

Port Range - Source Port typically ranges from 20000 to 40000 for TCP/UDP traffic. This range is used as the range of ports available for the source port of the traffic originating from the router and for the router to keep track of who originated the traffic from within the LAN. Normally 2 NAT rules must be created. One using the protocol of TCP/UDP and one using no protocol or port numbers. This is so ICMP traffic can traverse the router since ICMP traffic does not use port numbers.

6. NAT REDIRECT CONFIGURATION WINDOW

Delete	Add	Interface ID	Source		
			IP	Mask	Port
	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

Destination			Protocol
IP	Mask	Port	
<input type="text"/>	<input type="text"/>	<input type="text"/>	tcp

This page allows you to add or delete NAT redirections. This allows you to redirect traffic destined for specific ports of your WAN address to different machines on your local LAN. For instance if you wanted to run a web server on your local LAN accessible from the Internet.

Interface ID - Specify the interface across which the mapping occurs. Typically, the WAN interface.

Source - Source of mapped traffic. This would be the source address of the WAN interface with a 255.255.255.255 subnet mask and the particular destination port.

Destination - Destination of mapped traffic. This would be the IP address of the host on the LAN with a 255.255.255.255 subnet mask and the port you would like to forward traffic to

For example, you may have a FTP server in your LAN with an IP address of 192.168.1.16. You will have to map public access coming through your X320R,

with public address 209.141.176.154, to the internal PC. You would have a source address of 209.141.176.154 with a 255.255.255.255 mask and port of 21. Also, you would have the destination of 192.168.1.16 with a 255.255.255.255 mask and port of 21 if the server was using the standard FTP port.

Protocol - Transport protocol. Typically TCP/UDP

7. DHCP SUBNET CONFIGURATION WINDOW

Delete	Add	Subnet ID		Subnet Range	
		IP Address	Mask	From	To
<input type="checkbox"/>		192.168.1.0	255.255.255.0	192.168.1.200	192.168.1.249
	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

Default Gateway	Subnet Configuration Options			
	Default Lease Time	Max. Lease Time	Next Server IP	Server ID
192.168.1.1	10800	31536000	NULL	<input type="checkbox"/>
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

Subnet Configuration Options				
	Subnet Mask	Domain Name	Primary DNS	Secondary DNS
	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

This page allows you to configure the operation of the DHCP server. By enabling DHCP on your LAN, you do not have to assign a new IP address each time you add a PC to your network. This lets you avoid accidentally reassigning the same IP address or determining free addresses. Note: Each PC on you LAN must be configured as a DHCP client.

Subnet ID - Network ID. By default the X320R supports a network ID 192.168.1.0 with subnet mask 255.255.255.0.

Subnet Range - DHCP address pool. By default this is set to 192.168.1.200 to 192.168.1.249. The X320R supports a maximum of 50 DHCP clients.

Default Gateway - The is the default gateway your local LAN clients will use to access the internet. If using the default X320R setup, this would be set to 192.168.1.1 which is the X320R's local lan interface.

Default Lease Time - Format: seconds (10800 seconds = 3 hours). This value is the length of lease the router will normally give to DHCP clients.

Max Lease Time - Format: seconds (31536000 seconds = 365 days). This value determines what the max lease time the router will allow for a DHCP client. To differentiate between Default Lease Time and Max Lease Time, you can think of default lease time as the DHCP lease time the router will give to a DHCP client if the client doesn't specify a lease time. Max lease time is the maximum lease time the router will give to a DHCP client even if the client asks for a larger lease time.

Next Server IP - Next Server IP

Server ID - Address of DHCP server. Typically this option is not needed. This is normally the address of the DHCP server, which if using the X320R's default configuration would be 192.168.1.1

Subnet Mask - Subnet of DHCP server. Typically this option is not needed as it overrides the subnet mask that was configured earlier. This is normally the subnet mask of the DHCP server, which if using the X320R's default configuration would be 255.255.255.0 which is the subnet mask of the X320R's LAN interface.

Domain Name - This is the domain name that is going to be given to each DHCP client. Typically this is the same as the ISPs domain name. For instance the domain name for Xpeed is xpeed.com.

Primary DNS - This is the Domain Name Server that each DHCP client will use to resolve names. This would be given to you by your ISP

Secondary DNS - This is the Domain Name Server that each DHCP client will use to resolve names if there is no response to requests sent to the Primary DNS. This would be given to you by your ISP

8. ROUTE TABLE CONFIGURATION WINDOW

Delete	Add	Destination IP Address	Net Mask	Default Gateway	Metric	Static	Up
<input type="checkbox"/>		192.168.1.0	255.255.255.0	192.168.1.3	1	X	X
<input type="checkbox"/>		192.168.1.2	255.255.255.0	192.168.1.0	1	X	X
<input type="checkbox"/>		224.0.0.1	255.255.255.255	192.168.1.3	1		X
	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>			

This page allows you to modify the route table. Since entries are updated automatically, this page is recommended only for advanced users.

By default, the X320R is configured with the following

- LAN network ID entry
- PC's IP address entry
- Multicast entry

Destination IP address - is the destination host or network for which reachability information is to be added to the routing table

Netmask - is the mask that that is applied to the routing table entry that determines which range of addresses are defined by the routing entry

Default Gateway Gateway address through which the specified IP address/network can be reached

9. PASSWORD WINDOW

Enter Current Password :	<input type="password"/>
Select User Level	<input type="text" value="System"/>
Enter New Password :	<input type="password"/>
Re-Enter New Password :	<input type="password"/>

This page is used to change passwords on the X320R.

- Enter the current password
- Select the user access level:
 - System users have full read/write privileges
 - Guest users have only read privileges.
- Enter in the new password
- Re-enter new password for verification

10. DOWNLOAD FIRMWARE WINDOW

Select File or Enter Other File Name:	<input checked="" type="radio"/> x320_rt.img <input type="radio"/> Use the file below. <input type="text"/>
---------------------------------------	---

This page will allow you to reload or update the firmware on your X320R. The default file name is X320_rfw.imp. However, you can select another filename if different. Please also refer to Xpeed Quick Start for automatically retrieving and downloading the latest file from Xpeed.

11. REBOOT WINDOW

Some changes may require a reboot. To force the X320R to reboot itself, go to the reboot page and click on **Reboot**. You will have to log in to access the X320R again.

Chapter 6

Xpeed Command Line Interface

There are several ways to access the Command Line Interface on the X320R. You may use either a terminal emulation program or a TELNET session to access the X320R via a serial connection. Once you have accessed the X320R, you may configure the system using the CLI.

1. RS232 SERIAL INTERFACE

You may access your X320R through the serial port using any terminal emulation program. Connect a DB9 serial cable between the X320R and a PC running a terminal emulation program, such as HyperTerminal under Windows. However, any terminal emulation program will work using the settings below:

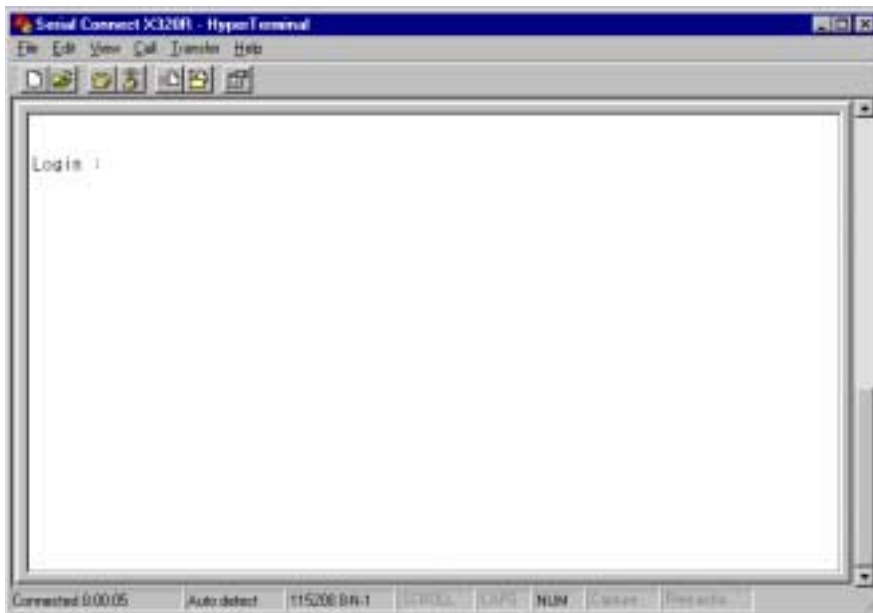
- Serial Connection Speed: 115200 bps
- Data Bits: 8
- Parity: None
- Stop Bits: 1
- Flow Control: None

Note: HyperTerminal may have Flow Control set to Hardware by default.

Once you open a new session on HyperTerminal, it will prompt you for the settings of your connection. Enter the settings as shown in the illustration below.



Once you have entered in the settings, HyperTerminal will display a terminal. Hit Enter to prompt the X320R. You will see the following Login prompt:



There are two different accounts available:

- **system** - allows administrative control over the X320R
- **guest** - allows the user to only view X320R settings

Please type **system** to login under the administrative account. Then type in your password (default is **system**). If you are successful, the X320R will prompt you with a ">".

At the prompt, you may enter any command available through the Command Line Interface (CLI). Descriptions of CLI commands are listed in the following section.

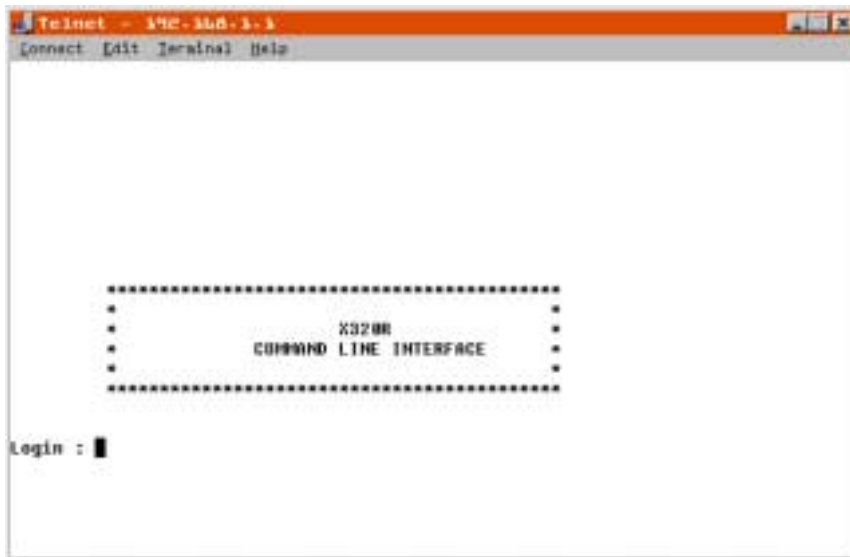
For quick help with commands, you can use the help command. If you type **help**, it will display a list of all the commands. You can also use **help** in context for

details on a particular command. For example, **help add** or **help add route**, will display detailed information respectively.

2. TELNET SESSION

You may open a TELNET session to configure and manage the X320R from anywhere on the network. This gives you the ability to modify your X320R without having to be directly connected to it.

In order to initiate a TELNET session, you must already have an Ethernet connection established between your X320R and the network. To access the X320R, use TELNET with the IP address of the X320R. For example, at a DOS command prompt, simply type “TELNET <IP Address>”. This will open a TELNET session in a TELNET window as shown below.



There are two different accounts available:

- **system** - allows administrative control over the X320R
- **guest** - allows the user to only view X320R settings

Please type **system** to login under the administrative account. Then type in your password (default is **system**). If you are successful, the X320R will prompt you with a “>”.

At the prompt, you may enter any command available through the Command Line Interface (CLI). Descriptions of CLI commands are listed in the following section.

For quick help with commands, you can use the help command. If you type **help**, it will display a list of all the commands. You can also use **help** in context for details on a particular command. For example, **help add** or **help add route**, will display detailed information respectively.

Chapter 7

CLI Commands

The X320R provides a Command Line Interface (CLI) for end-users who are more comfortable with configuring the X320R using a more powerful command interface. This section describes the purpose and usage of commands available through the CLI.

When using CLI commands, you do not have to type in the full command syntax. You can enter in enough of the command for the X320R to recognize what you have entered. For example, "show dhcpsubnet all" can be entered as "sh dh a". However, typing "sh d a" will be interpreted as an ambiguous by the X320R since "d" can be understood as either "dhcpsubnet" or "dslconfig" or "debuglevel".

Note:

Most commands require that the user "save" then "reboot" the router for the changes to take affect. The user will be prompted for these actions if needed.

Option fields separated by a "|" mean that either one of the options are valid but only one.

Option fields that include a " " can be ignored as they are just used to separate option fields used for ease of viewing.

Command option fields appearing within brackets “<>” signify input from the user and should not be included with the input from the user.

Command option fields appearing without “<>” around them are option flags that must be entered when using the option.

eg.

```
Add ArpEntry <IP Address> MACAddress <MAC Address>
```

user would type data in the form of:

```
add arpentry 192.168.1.250 MACAddress 0a:5b:d5:00:01:02
```

Note: as an alternate way to entering the full syntax of the commands users can use the interactive mode of the CLI whereby the user enters the command, presses the <enter> key, and is walked step-by-step through the available options. This is the preferred method of entering commands via the CLI. The full syntax of available commands are shown for completeness and not the ease of use factor of the interactive method. Example of using the interactive CLI is given below.

Example of interactive mode:

```
>add arpentry
```

output on screen

```
IPaddress:
```

user enters

```
192.168.1.200
```

output on screen

```
MAC Address:
```

user enters

```
0a:0b:0c:0d:0e:0f
```

1. ADD

Add command is used for adding new information about the option to the X320R.

ADD ARPENTRY

Adds an ARP entry into the X320R's ARP table. The entry takes effect immediately

Usage:

```
Add ArpEntry <IP Address> MACAddress <MAC Address>
```

<IP Address> is the address corresponding to specified MAC

<MAC Address> is the MAC address corresponding to specified IP address.

Example:

```
Add ArpEntry 192.168.1.100 MACAddress 0a:5b:6c:db:01:02
```

ADD DHCPSUBNET

Adds a DHCP subnet with specified parameters. This is the pool of addresses that the X320R assigns to DHCP clients requesting an IP address. Interactive mode is highly preferred for this command.

Usage:

```
Add dhcpsubnet <Subnet IP Addr>
Netmask <Subnetmask>
Range <From> <To>
<Default GW Addr>
Default-Lease-Time <Lease Time>
```

```

Domain-Name <Domain Name>
Domain-Name-Server <DNS1> <DNS2>
Max-Lease-Time <Max Lease Time>
Next-Server <Next Server>
Server-Identifier<Server Identifier>
Subnet-Mask <Netmask>

```

<Subnet IP Addr> is the subnet IP address of your LAN interface, this entry would be the network boundary of your DHCP subnet.

<Subnetmask> is the subnet netmask of your LAN interface.

<From> and <To> are the range limits of the address pool. <From> should be the lowest IP address. <To> should be the highest IP address. Note, the X320R supports a maximum of 50 DHCP clients.

<Default GW Addr> is the default gateway address, this entry should be the same as your X320R's LAN IP address.

<Lease Time> is the default DHCP lease time you wish your DHCP clients to use. Once a DHCP client is assigned an address this is the amount of time, in seconds, that the lease is valid before the DHCP client must re-request their original IP address or request an new address if the original address is unavailable. This option is not normally needed as the default is fine for most applications.

<Domain Name> is the domain name that your ISP uses. For example xpeed.com is the domain name for Xpeed.

<DNS1> and <DNS2> are the IP addresses of the Domain Name Servers your DHCP clients will use when resolving names to IP addresses. Most often you will only be given one of these but the option of having two is provided in case the first Domain Name Server becomes unavailable.

<Max Lease Time> is the maximum lease time, in seconds, that your X320R will allocate for DHCP clients even if the client requests a larger lease time in its DHCP request packet. This option is not normally needed for most applications.

<Next Server> This option is not normally needed for most applications.

<Server Identifier> specifies the IP address of the DHCP server which should be your X320R's LAN interface IP address. If this option is not used the X320R's LAN interface IP address is the default. This option is not normally needed for most applications.

<Netmask> This is the subnet mask that the DHCPclient is assigned. If no data is entered the subnetmask of the pool is assumed. This data was entered as the <Subnetmask> portion of the command listed above. This option is not normally needed for most applications.

For example if the DSL provider gave you the following information:

Domain name: isp.com

DNS server 1: 200.0.0.1

DNS server 2: 200.0.0.2

Then, if you were using the following configuration on your LAN interface:

L0 IP address of 192.168.1.1

L0 netmask 255.255.255.0

Finally if you knew that you wanted to configure the X320R for the maximum number of DHCP clients (50 DHCP clients), starting at 192.168.1.2 to 192.168.1.52 you would configure the X320R via either of the two following methods. The first method demonstrates using the full syntax of the command and the second method demonstrates using the interactive mode of the command.

Method 1 (full syntax of command is entered)

```
>add dhcpsubnet 192.168.1.0 netmask 255.255.255.0 range 192.168.1.2
    192.168.1.52 192.168.1.1 domain-name isp.com domain-name-server
    200.0.0.1 200.0.0.2
```

**** Please save configuration changes to permanent storage. ****

Method 2 (interactive mode)

>add dhcpsubnet

Subnet IP Address: 192.168.1.0

Subnet Netmask: 255.255.255.0

Subnet IP Address Range From: 192.168.1.2

Subnet IP Address Range To: 192.168.1.52

Default Gateway (IP Address): 192.168.1.1

Subnet Optional Parameters :

1. DEFAULT-LEASE-TIME
2. DOMAIN-NAME
3. DOMAIN-NAME-SERVER
4. MAX-LEASE-TIME
5. NEXT-SERVER
6. SERVER-IDENTIFIER
7. SUBNET-MASK
8. x-FINISHED

CHOICE : 2

Domain-Name (STRING): isp.com

Subnet Optional Parameters :

1. DEFAULT-LEASE-TIME
2. DOMAIN-NAME
3. DOMAIN-NAME-SERVER
4. MAX-LEASE-TIME
5. NEXT-SERVER
6. SERVER-IDENTIFIER
7. SUBNET-MASK
8. x-FINISHED

CHOICE : 3

Primary DNS (IP Address): 200.0.0.1

Secondary DNS (IP Address): 200.0.0.2

Subnet Optional Parameters :

1. DEFAULT-LEASE-TIME
2. DOMAIN-NAME
3. DOMAIN-NAME-SERVER
4. MAX-LEASE-TIME
5. NEXT-SERVER
6. SERVER-IDENTIFIER
7. SUBNET-MASK
8. x-FINISHED

CHOICE : 8

** Please save configuration changes to permanent storage. **

ADD FILTER

Defines a new IP filter. Filter rules allow IP traffic to either be blocked by the router or allowed to pass through. The filter rules enable the router to prevent unauthorized access to your LAN across the WAN link and also allows you to block unauthorized users from accessing resources outside of your LAN. The following full syntax is not given for the command as it is very difficult to add filters via the CLI although interactive method is preferred if the user still chooses to use the CLI. Therefore, it is highly recommended the filters be added via the WebGUI therefore a description of the available options and command usage is given in the IP filter section of the Web Interface section of the manual.

Usage:

Add Filter

Below is an example of using the interactive method to add a filter to block all local LAN users 192.168.1.2 - 192.168.1.52 from surfing the internet.

```
>add
  1. ARPENTRY
  2. DHCPSTNET
  3. FILTER
  4. INTERFACE
  5. NAT
  6. ROUTE
CHOICE : 3
FILTER GROUP NUMBER(Group Number(1-
8)|Group.Rule Number(1-8)) : 3
Action("Block"|"Pass") : block
"RETURN-ICMP"/"RETURN-RST"/"NONE" :
"IN"|"OUT" : out
Quick(Y|N) [N]: y
ON(Interface Name|"None") [None] : w0.0
DUP-TO(Interface Name:IP-Address|"None")
[None]:
TOS(Decimal Number (0 to 255)|"None") [None]:
TTL(0 to 255|"None") [None]:
Proto("TCP/UDP"|"UDP"|"TCP"|"ICMP"|"None")
[None]: tcp
Source and Destination("All"|"From") [All]:
from
From("any" | IP Address | Hostname) [any]:
192.168.1.0
Mask(IP Address | IP Address in Hex | "None")
[None]: 255.255.255.0
Want to filter against specific port number
(Y|N) [N]: n
To("any" | IP Address | Hostname) [any] : any
```

Want to filter against specific port number

(Y|N) [N]: y

1. !=

2. <

3. <=

4. =

5. >

6. >=

7. EQ

8. GE

9. GT

10. LE

11. LT

12. NE

13. PORT-RANGE

CHOICE : 4

Port Number (Number 0-65535): 80

TCP Flags/Flag

Mask('F'|'S'|'R'|'P'|'A'|'U'|"None") [None]:

With("With"|"And"|"None") :

Keep("State"|"Frag"|"None") [None]:

ADD INTERFACE

Defines a new Interface with the specified parameters. This command is only valid for WAN interfaces. This is due to the fact that only 1 LAN interface is allowed on the X320R and cannot be deleted. Note: if using PPP there can only be one WAN interface due to the nature of PPP.

Usage:

Add Interface <Interface>

DHCPClient <on|off>

```

DLCI <dlci#>
Enable <y|n>
FramingType <Framing>
Gateway <GW Addr>
IPAddress <IP Addr>
Netmask <Netmask>

```

<Interface> is the WAN interface to be configured, eg. W0.0

DHCPClient when enabled allows the WAN interface to dynamically obtain its IP address information from the DSL provider.

<DLCI#> is the Data Link Channel Identifier. It identifies the logical link(s) that traverses the physical WAN link. Your DSL provider would provide this information.

<Framing> describes how the SDSL frames are formatted. This must match what the DSLAM is using. Your DSL provider would provide this information. Valid options are:

```

IPRouting, i.e., RFC1490 IP Routing
BridgedEthernet
RFC1490MAC
RFC1483MAC

```

<GW addr> is the IP address of the gateway or default route used to access the Internet/Intranet. Can be left with 0.0.0.0 if using DHCPClient

<IP Addr> is the IP address of the WAN interface. Can be left 0.0.0.0 if using DHCPClient.

<Netmask> is the netmask used on the WAN interface. Can be left 0.0.0.0 if using DHCPClient.

Example:

```

add interface w0.0 dhcpclient off dlci 17 enable y framingtype iprouting gateway
205.10.5.1 ipaddress 205.10.5.2 netmask 255.255.255.0

```

ADD NAT

Adds a NAT rule with the specified parameters. Although the full syntax of the command is given it is highly recommended that the user configure NAT maps & redirects via the interactive method or Web GUI. Please see the web interface section of the manual to see a better explanation of NAT. Typically 2 NAT filters are added for NAT MAPS. One using the protocol of TCP/UDP and port numbers, and one using no protocol and no port numbers as this is needed so ICMP traffic can traverse the router correctly since ICMP packets do not use port numbers.

Usage:

```
Add nat <mapit> <ifname>
      <from IP addr> mask <mask>
      to <to IP addr> mask <mask>
      mapport <y/n>
      <protocol>
      <from port>
      to <to port>
```

<mapit> specifies map or redirect (MAP|RDR). You would add a map for local LAN traffic wanting to access the internet and you would add a NAT redirect if you wanted hosts on the internet to access services, ie. web server, on your local LAN.

<ifname> is the interface on which the NATing occurs. Typically this would be your WAN interface

<from IP addr> mask <mask> For NAT map this would typically be your local LAN network, ie. using the default configuration this would be 192.168.1.0 with a 255.255.255.0 subnetmask. For NAT redirects this would typically be the WAN interface with a 32 bit subnetmask of 255.255.255.255.

<to IP addr> mask <mask> For NAT map this would typically be your WAN IP address with a 255.255.255.255. subnet mask. For NAT redirects this would typically be your local LAN server that you want to forward WAN traffic to.

mapport Tells the X320R to include protocol information when doing a NAT. As was said earlier, you would normally create 2 almost identical NAT rules for NAT maps, one with mapport set as “y” and including protocol with port numbers typically ranging from 20000 to 40000 for source port numbers and another with mapport set as “n” including no protocol or port information for ICMP packets to traverse the router correctly.

<protocol> This can be set to either “udp”, “tcp”, or “tcp/udp”. Typically this is set to “tcp/udp” when doing mapport with NAT maps & redirects.

<from port> Typically set to 20000 when using NAT maps this value is what is set as the beginning of the available source ports of traffic leaving the WAN side when being initiated from the LAN side, ie when a user is surfing the internet. If using a NAT redirect this is set to the particular port number you would like to forward, ie. 80 for HTTP traffic you would like directed from the WAN side to the LAN side server.

<to port> Typically set to 40000 when using NAT maps this value is what is set as the last of the available source ports for traffic leaving the WAN side when being initiated from the LAN side, ie when a user is surfing the internet. If using a NAT redirect this is the particular port number your LAN side server is listening on, ie. if you were running a web server on port 80 on your LAN you would set this value to 80.

ADD ROUTE

Adds a new route in the route table.

Usage:

```
Add Route <IP Address> netmask <Netmask>
        gateway <GW Address>
```


<IP Address> is the network/host address for which reachability information is to be added to the routing table

<Netmask> is the mask that is applied to the routing table entry that determines which range of addresses are defined by the routing entry

<GW Address> Gateway address through which the specified IP address/network can be reached

Example:

Add Route 192.168.2.0 netmask 255.255.255.0 gateway 192.168.1.0

2. ALIAS

ALIAS

Alias provides an interface to customize strings of frequently used commands

Usage:

```
alias <alias name> <alias string>
```

<alias name> is the alias to be created/modified, supports up to 16 characters.

<alias string> is the string of words to be aliased, supports up to 32 characters.

Example:

```
alias allint show interface all
```

3. DELETE

DELETE ARPENTRY

Deletes ARP entry from the ARP table. The command becomes effective immediately.

Usage:

```
Delete ArpEntry <IP Address>
```

<IP Address> is the address whose MAC is to be removed from ARP Table

Example:

```
delete arpentry 192.168.1.100
```

DELETE DHCP SUBNET

Deletes a DHCP SUBNET from the the X320R.

Usage:

```
Delete DHCPSubnet [<Subnet IP Addr>  
netmask <Subnetmask>] | <All>
```

<Subnet IP Addr> is the subnet that the DHCP range is based off.

<Subnetmask> is the subnet netmask of the DHCP range.

<All> is the option to delete all DHCP subnet ranges configured on the router.

Examples:

```
delete dhcpsubnet 192.168.1.0 netmask 255.255.255.0
```

```
delete dhcpsubnet all
```

DELETE FILTER

Deletes the specified IP filter(s) from the X320R.

Usage:

```
Delete Filter rule [In|Out <WholeGroup#>|All] |  
[<WholeGroup#>|<Group#.Rule#>] | All
```

In specifies any rules that apply to incoming traffic to the X320R interfaces

Out specifies any rules that apply to outgoing traffic from the X320R interfaces

<WholeGroup#> specifies a specific rule group to delete. This deletes all of the in going or outgoing rules of the specified group, depending on whether the user selects “in” or “out” rules.

All specifies all the incoming or outgoing rules, depending on whether the user selects “in” or “out” rules

<WholeGroup#> specifies a specific rule group to delete. This deletes all of the “in” and “out” rules under the specific rule group

<Group#.Rule#> specifies a rule group number and specific rule to delete from the group .

All specifies all filters currently configured on the X320R.

Examples:

delete filter rule in 1	This deletes all incoming traffic rules from group 1
delete filter rule out all	This deletes all outgoing traffic rules from any group
delete filter rule 1	This deletes all the rules from group 1
delete filter rule 2.3	This deletes the 3rd rule from group 2

delete filter rule all This removes all of the rules from the X320R

DELETE INTERFACE

Deletes the specified interface. This command is only valid for WAN interfaces as the X320R only supports a maximum of 1 LAN interface and this interface cannot be deleted.

Usage:

Delete Interface <Interface>

<Interface> specifies the interface to be deleted.

Example:

```
delete interface w0.2
```

DELETE NAT

Deletes the specified NAT rule

```
Delete NAT rule <Rule#>|all
```

<Rule#> is the NAT rule number. This number can be 1-8.

all keyword instructs the router to delete all NAT rules from its NAT table.

Examples:

```
Delete NAT rule 2
```

```
Delete NAT rule all
```

DELETE ROUTE

Deletes specified route from the routing table.

Usage:

Delete Route <IP Address>

<IP Address> is the network route entry which is to be deleted.

Example

Delete route 10.0.0.0

4. DISABLE**DISABLE DEBUGLEVEL**

Disables debug mode on the router.

Usage:

disable debuglevel

DISABLE FILTER

Disables processing of traffic by the specified filter(s).

Usage:

Disable Filter rule [In|Out <WholeGroup#>|**All**] |
[<WholeGroup#>|<Group#.Rule#>] | All

In specifies any rules that apply to incoming traffic to the router interfaces

Out specifies any rules that apply to outgoing traffic from the router interfaces

All keyword specifies all the incoming or outgoing rules, depending on whether the user selects “in” or “out” rules

<WholeGroup#> specifies a specific rule group to disable. This disables all of the rules under the specific rule group

<Group#.Rule#> specifies a rule group number and specific rule to disable from the group.

All specifies all filters currently running on the router.

Examples:

disable filter rule in 1	This disables all incoming rules from group 1
disable filter rule out all	This disables all outgoing rules from any group
disable filter rule 1	This disables all the rules from group 1
disable filter rule 2.3	This deletes the 3rd rule from group 2
disable filter rule all	This disables all of the rules on the router

DISABLE MEMORY

Disables Show memory information

Usage:

Disable memory

5. ENABLE

ENABLE DEBUG

Enables debugging of the LAN & WAN interfaces.

Usage:

```
Enable debug ENET [<Y>|<N>] HDLC [<Y>|<N>]
```

ENET is for debugging on the LAN interface

HDLC is for debugging on the WAN interface

ENABLE DEBUGLEVEL

Sets the amount of debugging information that is provided to the user.

Usage:

```
Enable Debuglevel <level>
```

<Level> specifies the detail of information available to the user. Valid options:

- <1> specifies some information
- <2> specifies most information
- <3> specifies all information

ENABLE FILTER

Enables processing of traffic by the specified filter(s).

```
Enable Filter rule [In|Out <WholeGroup#>|All] |  
[<WholeGroup#>|<Group#.Rule#>] | All
```

In specifies any rules that apply to incoming traffic to the router interfaces

Out specifies any rules that apply to outgoing traffic from the router interfaces

All Specifies all the incoming or outgoing rules, depending on whether the user selects “in” or “out” rules

<WholeGroup#> specifies a specific rule group to enable. This enables all of the rules under the specific rule group

<Group#.Rule#> specifies a rule group number and specific rule to enable from the group.

All specifies all filters currently configured on the X320R

Examples:

enable filter rule in 1	This enables all incoming rules from group 1
enable filter rule out all	This enables all outgoing rules from any group
enable filter rule 1	This enables all the rules from group 1
enable filter rule 2.3	This enables the 3rd rule from group 2
enable filter rule all	This enables all of the rules on the router

ENABLE MEMORY

Sets the show memory information time interval.

Usage:

Enable memory <time>

<time> specifies the show memory interval in seconds

6. HELP

HELP

Help provides information and usage of commands supported by the system

Usage:

Help [command [sub-command]]

For Example:

>help add

Add command adds entries to tables.

It accepts the following input parameters:

- 1) ARPEntry: Add entries to the ARP table.
- 2) DHCPSubnet: Add DHCP subnet(s).
- 3) Filter: Add IP filter rule(s).
- 4) Interface: Add LAN, or WAN interfaces.
- 5) NAT: Add NAT rule(s).
- 6) Route: Add entries to the route table.

>help add arpentry

Adds ARP entry to the ARP table.

Usage:

Add ArpEntry <IP Address> MACAddress <MAC Address>
 where <IP Address> is the address for which corresponding MAC
 is being specified
 <MAC Address> is the MAC address of the machine
 configured with specified IP address

7. IPCONFIG

IPCONFIG

Displays ipconfiguration information for the LAN & WAN interfaces.

Usage:

```
ipconfig <interface>
```

<Interface> specifies the interface the user wishes to display IP information on

Example:

```
ipconfig w0.1
```

```
ipconfig l0
```

8. LOGOUT

LOGOUT

Logout terminates the user session; equivalent to the exit and quit commands.

Usage:

```
Logout
```

9. MODIFY

MODIFY COMMUNITY

Modifies the SNMP community string.

Usage:

```
Modify Community <string>
```

<string> specifies the public community SNMP string for the router

MODIFY CONSOLE

Modify Console facilitates changing maximum number of rows to be displayed on the screen

Usage:

```
Modify Console <rows>
```

<rows> specifies the maximum number of rows to be displayed at a time.
The values can range from 1-20 rows.

MODIFY DEVICE

Modify device changes the mode of the device to perform as a router or as a bridge

Usage:

```
Modify Device [bridge|router]
```

MODIFY DSLCONFIG

Modify DSLConfig modifies the DSL configuration of the selected WAN interface

Usage:

```
Modify DSLConfig <Interface>  
    LinkSpeed <Speed>  
    SerialSwapped (y|n)  
    StreamInverted (y|n)
```

<Interface> is the port to be configured, i.e. W0.0

<Speed> is the speed of your service, autosense is the default.

SerialSwapped please refer to the description on QuatSwap in the Trouble Shooting section to determine if this is to be enabled.

StreamInverted please refer to the description on InvertedBits in the Trouble Shooting section to determine if this is to be enabled.

Example:

```
Modify DSLConfig W0.0 LinkSpeed 784 serialswapped Y
streaminverted Y
```

MODIFY FRCONFIG

Modifies the Frame Relay parameters for the specified interface.'

Usage:

```
Modify FRConfig <Port>
    LMI [on|off]
    Switchtype [ANSI|q.933]
    Termination [lt|nt]
```

<Port> is the port to be configured, currently only W0 is supported

LMI is the link management interface, default is off, DSL provider would determine if this is enabled or disabled.

Switchtype is typically set to ANSI for users in the United States or q.933 for users in Europe

Termination is the termination type. This can be set to lt for line termination or nt for network termination. For most users this should be set to NT (Network Termination) . If doing back to back with X320Rs one X320R

must be set to LT (Line Termination) and one X320R must be set to NT (Network Termination).

Example:

```
modify frconfig w0 lmi on switchtype ansi termination nt
```

MODIFY INTERFACE

Modifies the parameters of the configured interface.

Usage:

```
Modify Interface <Port>
    DHCPClient on|off
    DHCPServer on|off
    FramingType <Framing>
    Gateway <GW Addr>
    IPAddress <IP Addr>
    Netmask <mask>
```

<Port> is the interface to be configured, ie. W0.0 or L0

DHCPClient this option is only available when configuring a WAN interface. Enabling this feature allows the X320R to obtain its IP address for it's WAN interface via the DSL connection.

DHCPServer this option is only available when configuring a LAN interface. Enabling this feature allows the X320R to act as a DHCP server thus, handling DHCP address assignments for the clients on the LAN.

Enable option selects whether the interface is enabled or disabled.

<Framing> is only available when configuring a WAN interface. This selection determines the framing type used on the DSL link

Valid Options are:

IPRouting, i.e. RFC1490 IP Routing

BridgedEthernet, i.e. RFC 1490 Bridged Ethernet

RFC1490MAC,

RFC1483MAC

<GW Addr> is only available when configuring a WAN interface. This address is the default gateway of the router.

<IPAddress> is the IP address of the specified interface.

<Netmask> is the netmask of the specified interface.

Examples:

```
>modify interface w0.0 gateway 2.2.2.2 ipaddress 2.2.2.2 netmask 255.255.255.0
```

**** Please save and reboot for changes to take effect. ****

An example of using the modify interface with interactive mode is given below:

```
>modify interface <enter>
Interface: w0.0 <enter>
Dhcp Client (ON|OFF) [OFF]: <enter>
Enable (Y|N) [Y]: <enter>
FramingType (IPRouting|BridgedEthernet|RFC1490MAC|RFC1483MAC) [IPRouting]:
RFC1483MAC <enter>
Gateway [0.0.0.0]: 172.18.15.81 <enter>
IPAddress [0.0.0.0]: 172.18.15.90 <enter>
Netmask [0.0.0.0]: 255.255.255.240 <enter>

>reboot <enter>
Reboot [N]: y <enter>
Rebooting...
```

Note:

In the above example, 172.18.15.81 is the IP address of DSLAM, 172.18.15.90 is X320R's WAN IP address.

MODIFY PPPCONFIG

Modifies the PPP configuration on the X320R..

Usage:

```
Modify PPPConfig <interface>
    Authentication [AUTO|CHAPONLY]
    ChapType [MD5|MSCHAP]
    Enabled [Y|N]
    HeaderCompression [y|n]
    Userid <String>
    Userpw <String>
```

<interface> refers to the WAN interface you wish to configure. ie. w0.0

Authentication refers to the type of authentication method you wish to use.

The available options are **Auto** and **Chaponly**

ChapType refers to type of Challenge Handshaking Authentication Protocol you wish to you. The available options are **MD5** and **MSCHAP** (Microsoft)

Enabled either enables or disables PPP on the selected WAN interface.

HeaderCompression determines if the user is going to be using IP header compression on the selected interface.

Userid is the user's PPP userID

Userpw is the user's PPP User password.

MODIFY RIP

Modifies RIP, configuration on the X320R..

Usage:

```
Modify RIP [LAN|WAN]  
        Receive [y|n]  
        Send [y|n|<broadcast>|<unicast>]
```

<LAN> configures RIP on the LAN interface.

<WAN> configures RIP on the WAN interface.

Receive enables the X320R to receive and process RIP (version 1 or 2) routing information.

Send enables the X320R to transmit RIP (version 2) routing information to other routers. The *Broadcast* and *Unicast* options are only available on the WAN interface.

Examples:

```
modify rip lan receive y send y
```

```
modify rip wan receive y send broadcast
```

MODIFY TRAPIPADDR

Modifies the IP address that the router sends SNMP trap information to

Usage:

```
Modify Trapipaddr <IPaddress>
```

<IPaddress> is the address of the SNMP trap collection station

Example:

```
modify trapipaddr 192.168.1.254
```

10. PASSWORD

PASSWORD

Password command facilitates changing passwords for both the system (Read-Write user) and guest (Read-Only users) user. The password for either users can only be modified by the System (Read-Write) user.

Usage:

```
Password
```

Note: The command works only in interactive mode. When the user is given the *Password:* prompt the user must enter the current *system user* password. Once this is entered the user is prompted with the the following line:

Level [system / guest] :

The user must now select which password they wish to change. Once this level user is selected, the user is prompted to enter the new password for this level user. Once this is entered the user is again prompted to type the password in again to verify the user did not make an error typing the password the first time

Example:

```
>password
```

```
Password :
```

```
Level [system | guest] :guest
```

New Password :

Re-Type Password :

Note: When typing in the passwords it is hidden from the user for security reasons.

11. PING

PING

Ping command can be used by the user to determine reachability to specified IP address

Usage:

```
Ping <Destination-IP>  
    Count <Number>  
    Timeout <Number-of-Seconds>
```

<Destination-IP> is the specified IP you are trying to reach

<Number> is the number of times to ping the specified IP address

<Number-of-Seconds> is the number of seconds to wait on a ping reply before determining that the IP address is deemed unreachable.

Example:

```
Ping 10.1.0.2 count 5 timeout 10
```

12. QUIT

QUIT

Quit terminates the user session; equivalent to the exit and logout commands.

Usage:

Quit

13. REBOOT

REBOOT

Reboots the system

Usage:

Reboot

14. RESTORE

RESTORE

Restores the default configuration

Usage:

Restore

15. SAVE

SAVE

Saves the current configuration to non-volatile memory.

Usage:

Save

16. SHOW

Show displays the configuration of the system. Various sub-parameters supported by show are:

SHOW ALL

Displays the complete system configuration.

Usage:

show all

SHOW ARP

Displays the entries of ARP table.

Usage:

show arp

SHOW COMMUNITY

Displays the SNMP public community string of the X320R.

Usage:

show community

SHOW CONSOLE

Displays the configuration settings for the console port.

Usage:

```
show console
```

SHOW DEBUGLEVEL

Displays the current debug level configured on the X320R.

Usage:

```
show debuglevel
```

SHOW DEVICE

Displays what mode the X320R is operating in, either router or bridge.

Usage:

```
show device
```

SHOW DHCP SUBNET

Displays which DHCP pools are setup within the X320R..

Usage:

```
show dhcpsubnet [<subnetnetwork> netmask <subnet-  
mask>] | <all>
```

<subnetnetwork> is the network ID of the dhcpsubnet pool.

<subnetmask> is the subnet mask of the dhcpsubnet pool

<all> displays all defined dhcp address pools

Examples:

```
show dhcpsubnet 192.168.1.0 netmask 255.255.255.0
```

```
show dhcpsubnet all
```

SHOW DSLCONFIG

Displays DSL parameters of configured ports.

Usage:

```
show dslconfig <interface>
```

<interface> is the WAN interface you wish to display information about, ie.
w0

SHOW FILTER

Displays filtering information.

Usage:

```
show Filter [packet state|frag state|statistics]
```

or

```
show Filter rule [In|Out <WholeGroup#>|All] |
[<WholeGroup#>|<Group#.Rule#>] | All
```

packet state specifies information on the types of packets that the filtering process has processed.

frag state specifies information on fragmented packets the X320R has processed.

statistics specifies information about the whole filtering processes

In specifies any rules that apply to incoming traffic to the router interfaces

Out specifies any rules that apply to outgoing traffic from the router interfaces

All Specifies all the incoming or outgoing rules, depending on whether the user selects “in” or “out” rules

<WholeGroup#> specifies a specific rule group to display information about.
This displays all of the rules under the specific rule group

<Group#.Rule#> specifies a rule group number and specific rule to display information about.

All specifies all filters currently configured on the X320R

Examples:

show filter statistics	This displays information on the filtering process.
show filter rule in 1	This displays all incoming rules from group 1
show filter rule out all	This displays all outgoing rules from any group
show filter rule 1	This displays all the rules from group 1
show filter rule 2.3	This displays the 3rd rule from group 2
show filter rule all	This displays all of the rules on the router

SHOW FRCONFIG

Displays FR parameters of the selected port

Usage:

```
show frconfig <interface>
```

<interface> is the WAN interface you wish to display information about, ie.
W0

SHOW INTERFACE

Displays parameters of the selected interface.

Usage:

```
show interface <interface>
```

<interface> is the interface you wish to display information about, ie. W0.0,
L0

SHOW MEMORY

Displays the the memory information & uptime of the router.

Usage:

```
show memory
```

SHOW NAT

Displays NAT rules configured on the router.

Usage:

```
show NAT <statistics>|[rules <rulenum>|<all>]
```

<statistics> specifies usage statistics of all the rules

rules specifies that you wish to view a specific NAT rule

<rulenum> specifies the exact NAT rule you wish to display information on.

<all> specifies you wish to display all of the configured NAT rules

SHOW PPPCONFIG

Displays the the PPP configuration information.

Usage:

```
show PPPConfig <interface>
```

<interface> specifies the WAN interface you wish to display PPP configuration info on.

SHOW MEMORY

Displays the the memory information & uptime of the router.

Usage:

```
show memory
```

SHOW RIP

Displays the RIP configuration.

Usage:

```
show rip
```

SHOW ROUTE

Displays the routing table.

Usage:

```
show route
```

SHOW SYSCONFIG

Displays information on the router such as the production date, HW version, SW version, serial number, and uptime .

Usage

```
show sysconfig
```

SHOW TRAPIPADDR

Displays the IP address that the router forwards SNMP trap information.

Usage:

```
show trapipaddr
```

17. TFTP

TFTP

Transfers files from a remote computer running the TFTP service.

Usage:

```
TFTP <source-IP> GET <filename>
```

<Source-IP> IP address of TFTP server.

GET Transfers the file from TFTP server to the X320R.

<filename> Name of file to be transferred to the X320R.

18. TRACEROUTE

TRACEROUTE

TraceRoute facilitates determining route to specified internet destination

Usage:

```
TraceRoute <destination-IP-Address>
```

<destination-IP-Address> is the address of the station/router you are trying to reach.

19. UNALIAS

UNALIAS

Delete existing alias created by 'alias' command

Usage:

```
Unalias <aliased-word>
```


Chapter 8

IP Networking Basics

This section will provide you with an overview of IP networking concepts. If you are new to the subject, this section will help you understand some of the concepts and materials presented throughout the User's Guide. You may also refer to the Glossary for additional reference.

1. WHAT IS A ROUTER?

A router is a device that routes traffic between networks based on information in the network layer of a packet and routing tables maintained by the router. The router maintains the routing table by exchanging routing information with other routers in the network. Using the information provided by the routing table, the router is able to determine the best path for directing network traffic.

Routing Information Protocol (RIP) is one type of routing protocol used by a router to build and maintain a map of the network. A router uses RIP to regularly update itself and check for any changes to the routing table. RIP1 and RIP2 are both supported by the X320R, although the X320R only transmits RIP2 version packets.

Routers can vary in size and performance. The Xspeed 320R is a small office router supporting IP routing between a DSL line and a Local Area Network (LAN). It allows optimization of IP traffic between the LAN and the WAN.

In addition, routing improves network security by isolating traffic to the LAN. The X320R will prevent information intended for recipients in your local network from going out externally.

2. IP ADDRESSING

Every PC has a unique IP address assigned to it to ensure that data reaches the correct destination. The IP address is a 32-bit structure, typically written in a dot notation with 8-bit groups. For example the IP address:

192.168.1.15

represents a 32-bit structure:

11000000 10101000 00000001 00001111

An IP Address consists of two parts: a network identifier and a host identifier. The dividing point may vary, depending on the addressing class or subnet being used. There are five standard addressing classes:

- Class A - uses an 8-bit network address and a 24-bit host address. This allows up to 16,777,214 hosts on each network.
- Class B - uses a 16-bit network address and a 16-bit host address. This allows up to 65,354 hosts on each network.
- Class C - uses a 24-bit network address and an 8-bit host address. This allows up to 254 hosts on each network.
- Class D - is used for multicast
- Class E - is for experimental use.

For each network address range, there are two addresses that are reserved:

- Host Address is all 0s - Network address used to identify the network, not assigned to any host
- Host Address is all 1s - Broadcast address to send a packet simultaneously to all hosts with the same network address.

3. NETMASK

The netmask allows you to identify the network and host portions of an address without knowing the address class. The netmask is a 32-bit number, expressed in dot-notation, that is logically ANDed with the IP address to yield the network address.

The IP address classes have corresponding netmasks:

- Class A - 255.0.0.0
- Class B - 255.255.0.0
- Class C - 255.255.255.0

For example, the IP address 192.168.1.15 is a Class C address broken down as follows:

IP Address

11000000.10101000.00000001.00001111 (192.168.1.15)

Netmask

11111111.11111111.11111111.00000000 (255.255.255.0)

ANDed

11000000.10101000.00000001.00000000 (192.168.1.0)

Where 192.168.1.0 is the IP address identifying the network.

4. SUBNET

Subnet addressing allows a network to be split into smaller subnetworks. For example, if a Class C network address is assigned to a small company, it may be unlikely for that company to use all 254 host addresses. Instead, the 254 host network may be divided into several smaller subnets. A company can then assign subnets to individual departments or floors, dividing the network logically into easily manageable groups.

ISPs also use subnets to assign a range of IP addresses for a business customer. A Class C network with 256 addresses can be divided into 32 subnets each with 8 host addresses. Note that two of those addresses can not be used. This is due to the fact that the first address in each subnet is the network address of the subnet and the last address in each subnet is the broadcast address of that subnet. This allows the ISP to effectively support 32 small businesses with multiple IP addresses.

The subnet used in this example is as follows:

11111111.11111111.11111111.11111000 (255.255.255.248)

The last three bits are left blank, allowing for 8 host IP addresses.

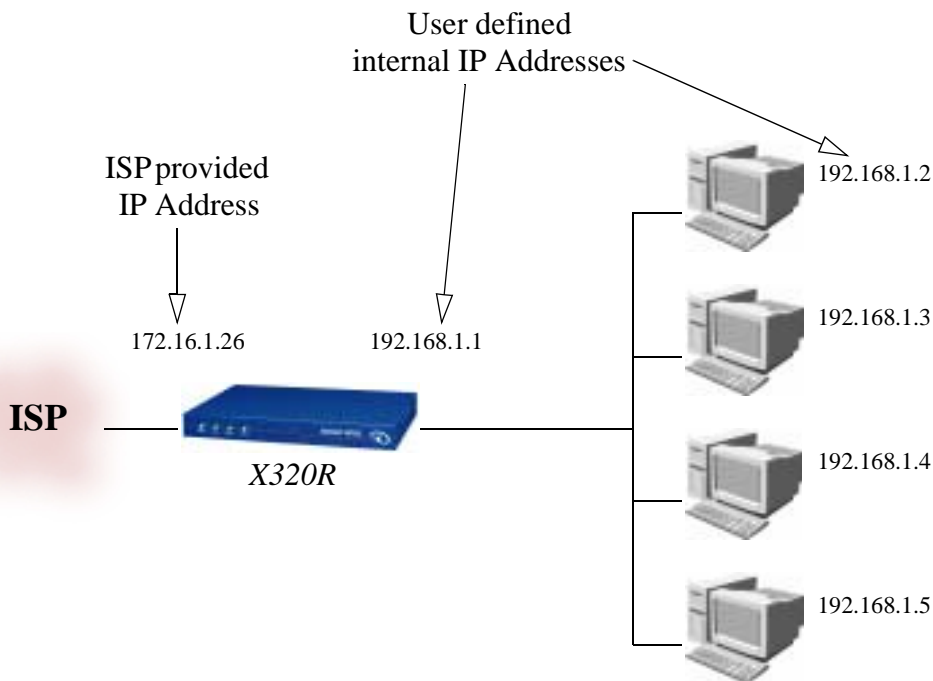
Typically, all hosts on a LAN segment will use the same subnet. This allows all the hosts to recognize local IP broadcasts, and allows the router to differentiate between local and remote addresses.

5. NETWORK ADDRESS TRANSLATION

Typically, you will deal with two sets of IP addresses. One or more IP addresses will be assigned to you by your ISP. This will be referred to as the WAN IP address. Another set of IP addresses will be used in your LAN; each host on your LAN will have its own IP address. The LAN and WAN IP addresses are independent of each other, if you are using a feature called Network Address Translation (NAT) which allows you to map LAN addresses to the WAN. A key benefit of NAT is the ability to map multiple LAN addresses to a single WAN IP address, a feature commonly known as line-sharing.

Traditionally, the way that ISPs supported line-sharing was to assign a block of IP addresses. However, NAT allows multiple users to share a single IP address, which may be assigned statically or dynamically by the ISP.

NAT works by translating the internal IP addresses to a single global address as illustrated below.



In the illustration, the ISP has assigned the user a single IP address of 172.16.1.26. The user, however, has several PCs in his network. He has defined his network address to be 192.168.1.X, where 192.168.1.1 is reserved for the X320R. The network may support up to 253 PCs with addresses ranging from 192.168.1.2 to 192.168.1.254.

The mapping property of NAT also provides firewall-like security since outside users, via the Internet, can not see into your internal network. They can only see

the address 172.16.1.26. On the inside, the PCs use the X320R as a gateway to go out onto the Internet.

6. LAN ADDRESS ASSIGNMENT

When using NAT, LAN addresses are independent of WAN addresses allowing the user much freedom in assigning addresses to the internal network. In some cases the user may opt to use DHCP, so that all PCs are assigned IP addresses automatically. This may be desired if PCs are added to or removed from the network frequently.

In the illustration describing NAT, the user had defined a network with the network address 192.168.1.X. The Internet Assigned Numbers Authority has reserved several blocks of addresses for use in private networks. It is recommended that you select your network address from one of the blocks below:

- **10.0.0.0 to 10.255.255.255**
- **172.16.0.0 to 172.31.255.255**
- **192.168.0.0 to 192.168.255.255**

Your selection of an internal subnet should be based on the expected size and complexity of your network.

7. MISCELLANEOUS

IP, or Internet Protocol, as used in this User's Guide is understood to refer to IPv4 as defined by RFC 791.

8. MORE INFO

For more information on IP networking, please refer to any of the several books on the subject including *Interconnections Second Edition: Bridges, Routers*,

Switches and Internetworking Protocols, by Radia Perlman, published by Addison-Wesley.

Chapter 9

Sample Application

The X320R has the flexibility to support a variety of configurations. However, most users do not require the full set of features. This section will describe the steps to getting your X320R up and running as quickly and easily as possible.

1. SMALL OFFICE PROFILE

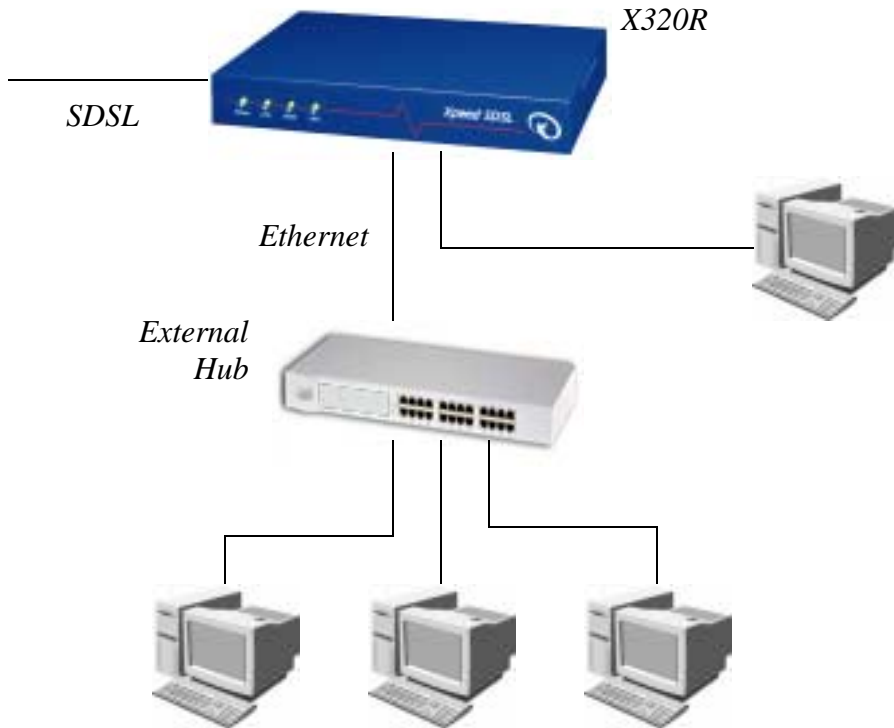
Number of Users: *1 to 253*

Usage: *Shared access; email server; web-site hosting*

Features: *NAT, Line Sharing*

Small office line-sharing is the most common application for the X320R, where multiple users are able to share a single high speed connection to the Internet. In addition to small offices, this application may also be used for SOHO, telecommuter and even home network environments where parents may want to share Internet access with their children.

This application can be scaled very easily, new users are added to the LAN by plugging into the hub. If not enough space is available on the hub, an additional hub may be added to expand capacity.



2. DHCP

Adding new PCs to your network is easy, especially if you are using Dynamic Host Configuration Protocol (DHCP). This allows the X320R to automatically assign an IP address dynamically to all the PCs on the LAN. Anytime a new PC is added to the LAN it will receive a new IP address allowing it to communicate with the rest of the network.

Note: The X320R will support a maximum of 50 DHCP clients.

3. HOW TO SET IT UP

For a home user with just one PC connected to the Internet via the Xpeed box, the connection is rather simple.

By default the X320R is configured with the following settings:

- LAN IP: 192.168.1.1
- LAN Subnet: 255.255.255.0
- DHCP Server: On.
- NAT Rules: on.

1. Add the PC to the network

- a) Connect an Ethernet cable from one of the X320R Ethernet ports to the PC.
- b) Set the PC to DHCP - also set the DNS Address supplied by your ISP.

2. Access the X320R

- a) To use the serial port, connect a serial cable from the DB9 connector on the Xpeed 320R to your a COM port on your PC.
- b) Open a HyperTerminal session on your PC. Please refer to the section on CLI for details on connecting to the serial port.

3. *Login as System user.*

Note: To configure the WAN port, you will need to know the IP address, unless DHCP client is being used on the WAN port, and account settings provided to you by your ISP.

4. Change the Frame Relay parameters.

- a) Type Modify

- b) Select the number for **FRCONFIG**
 - c) For **port** enter w0 for WAN interface
 - d) For **LMI** enter setting provided by your ISP
 - e) For **SwitchType** select ANSI
 - f) For **Termination** select NT
5. Change the DSL parameters.
- a) Type **Modify**
 - b) Select the number for **DSLCONFIG**
 - c) For **port** enter w0
 - d) For **Link Speed** select the setting provided by your ISP
 - e) For **Serial Swapped** select the setting provided by your ISP
 - f) For **Stream Inverted** select the setting provided by your ISP
6. Configure the IP addresses of your WAN port.
- a) Type **Modify**
 - b) Select the number for **Interface**
 - c) For **Interface** select an interface number. This interface has to be in the form of Wm.n ($0 \leq a \leq 3$, $m = 0$, $0 \leq n \leq 14$). For example W0.0 would be a valid interface number.
 - d) For **DHCP Client** select **Off**
 - e) For **Enable** select **Yes**
 - f) For **Framing Type** select the setting provided by your ISP
- Note: if using DHCP Client on the WAN port the user can accept the default settings of 0.0.0.0 for the IP Address, Netmask, and Default Gateway as these fields will be unused when DHCP client is active.
- g) For **Gateway** use the address provided by your ISP
 - h) For **IP Address** use the address provided by your ISP

- i) For **Netmask** use the address provided by your ISP)
- 7. The final configuration is to set the Network Address Translation (NAT) rule. First check that there are no NAT rules set.
 - a) Type `show`
 - b) Select the number for **NAT**
 - c) Type `rules`
 - d) Type `all`
- 8. If there are any rules then delete them using the following procedure:
 - a) Type `delete`
 - b) Select the number for NAT
 - c) Type `all`
- 9. Now add two new NAT rules for your connection.
 - a) Type `add`
 - b) Select the number for NAT
 - c) Type `map`
 - d) For **Interface Name** type `w0.0`
 - e) For **Original IP Address** type `192.168.1.1`
 - f) For **Mask IP Address** type `255.255.255.0`
 - g) For **To Mask Original IP Address** type `<WAN IP address in step 6>`
 - h) For **Mask IP Address** type `255.255.255.255`
 - i) For **Mapport** type `y`
 - j) For the **Mapport** selection type `TCP/UDP`
 - k) For the **From Port** type `20000`
 - l) For the **To Port** type `40000`
 - m) Type `add`

- n) Select the number for NAT
 - o) Repeat the above procedure, except type **n** for **Mapport** in step i. This step is needed for ICMP traffic to traverse the router correctly as ICMP packets do not use ports.
 - p) Save and reboot your router.
10. Verify that you have two link lights on: Power and Link. If not, then check your physical connections (i.e. cabling and power).
11. You should now be able to browse the internet!!!

4. TO ADD MORE USERS

You can add more PCs to your router by either using static or DHCP (dynamic) addresses, simply use the default settings.

To use Static addressing, you can use the following IP addresses:

PC#2

- IP: 192.168.1.5
- Mask: 255.255.255.0
- Gateway: 192.168.1.1

PC#3

- IP: 192.168.1.6
- Mask: 255.255.255.0
- Gateway: 192.168.1.1

etc...

Note: You can have as many PC as allowed by your subnet, by default 253 hosts. Also, the 320R only supports a maximum of 50 DHCP clients.

5. RUNNING A WEB SERVER ON YOUR LOCAL LAN

For example say you wanted to run a web server on your local LAN so clients on the internet could go your your website. Assume the following had the following network configuration and the router was already configured from the previous steps:

WAN interface: w0.0

WAN IP address: 216.5.4.1

WAN Mask: 255.255.255.0

LAN IP address: 192.168.1.1

LAN mask: 255.255.255.0

Local LAN server: 192.168.1.10

Local LAN server that is listening for web traffic: 80

To add a NAT redirect you would follow the steps below:

- a) Type **add nat**
- b) For **"MAP"|"RDR"** type RDR
- c) For **INTERFACE NAME** : type w0.0
- d) For **FROM MASK ORIGINAL IP ADDRESS** type 216.5.4.1
- e) For **MASK IP ADDRESS:** type 255.255.255.255
- f) For **Port(Decimal Number (0 to 65535))** : type 80
- g) For **TO MASK ORIGINAL IP ADDRESS** type 192.168.1.10
- h) For **MASK IP ADDRESS:** type 255.255.255.255

- i) For **Port(Decimal Number (0 to 65535))** : type 80
- j) For ("**UDP**"|"**TCP**"|"**TCP/UDP**") type tcp/udp
- k) Save your settings and reboot the router

Users should not be able to access your webserver from the internet!

6. PREVENTING USERS FROM SURFING THE INTERNET

For example say you wanted to prevent local LAN users from surfing the Internet. Due to the complexity of adding filters please refer to the web gui section for a full understanding of the filtering process. Assume your network had the following network configuration and the router was already configured from the previous steps:

WAN interface: w0.0

WAN IP address: 216.5.4.1

WAN Mask: 255.255.255.0

LAN IP address: 192.168.1.1

LAN mask: 255.255.255.0

LAN users: 192.168.1.2 - 192.168.1.52

To add a NAT rule to accomplish this would would complete the following steps:

- a) Type **add filter**
- b) For **FILTER GROUP NUMBER(Group Number(1-8)|Group.Rule Number(1-8))** : type 3.1
- c) For **Action("Block"|"Pass")** : type block
- d) For **"RETURN-ICMP"/"RETURN-RST"/"NONE"** : hit the enter key to accept none

- e) For **"IN"|"OUT"** : type out
- f) For **Quick(Y|N) [N]**: type y
- g) For **ON(Interface Name|"None") [None]** : type w0.0
- h) For **DUP-TO(Interface Name:IP-Address|"None") [None]**: hit the enter key to accept none
- i) For **TOS(Decimal Number (0 to 255)|"None") [None]**: hit the enter key to accept none
- j) For **TTL(0 to 255|"None") [None]**: hit the enter key to accept none
- k) For **Proto("TCP/UDP"|"UDP"|"TCP"|"ICMP"|"None") [None]**: type tcp
- l) For **Source and Destination("All"|"From") [All]**: type from
- m) For **From("any" | IP Address | Hostname) [any]**: type 192.168.1.0
- n) For **Mask(IP Address | IP Address in Hex | "None") [None]**: type 255.255.255.0
- o) For **Want to filter against specific port number (Y|N) [N]**: type n
- p) For **To("any" | IP Address | Hostname) [any]** : hit the enter key to accept any
- q) For
 - 1. !=
 - 2. <
 - 3. <=
 - 4. =
 - 5. >
 - 6. >=
 - 7. EQ
 - 8. GE
 - 9. GT

10. LE

11. LT

12. NE

13. PORT-RANGE

Type 4

- r) For **Port Number (Number 0-65535)**: type 80
- s) For **TCP Flags/Flag Mask('F'|'S'|'R'|'P'|'A'|'U'|"None") [None]**: hit enter to accept none
- t) For **TCP Flags/Flag Mask('F'|'S'|'R'|'P'|'A'|'U'|"None") [None]**: hit enter to accept none
- u) For **Keep("State"|"Frag"|"None") [None]**: hit enter to accept none
- v) Save the configuration and reboot the router for changes to take effect.

Users should now be unable to surf the internet but are still able to access any local web servers.

Appendix A

Trouble Shooting

- **I tried powering up my modem and the "power" LED does not come on.**

Verify that the power supply shipped with the X320 (AC/DC converter 9V, 1.5A) is plugged into a power outlet as well as the modem. If the modem is connected, the power light should immediately come on. If it does not, please contact Xpeed technical support.

- **The modem powers up, and the Link light is lit but I can not transfer data.**

Make sure that a good Ethernet cable is connected between any of the Ethernet ports on the X320 and the Ethernet port on your PC. Also confirm that your PC's Ethernet port has been configured correctly. You may need to consult your manuals provided with your Ethernet card.

Failure on any of the equipment in the service provider's network or backbone can also cause your data not to transmit. You can try to type "ping www" to verify if you can ping your gateway. If you can ping your gateway, the problem is likely congestion on the network. If you are not able to ping your gateway, double check your cables and contact your ISP.

Finally, confirm that the X320 Link protocol and speed are configured correctly.

- **I finished the installation of the modem, but I can't access the Internet. I noticed that the "link" light is off.**

The link light shows the status of the SDSL connection between the modem and your ISP. If this light is off, there is no DSL connection. Verify that the modem is connected to your SDSL line. If this link light does not come on within five minutes, either your service has not been enabled, or there is a problem with your SDSL speed and protocol settings. Contact your service provider to confirm that the service has been turned on and that our configuration settings are correct.

- **I finished the install for the modem, the link light is on, but I still can't access the Internet.**

Confirm that you have the Ethernet connection to the modem connected and configured correctly. If you have a good DSL connection (link light is on), a good Ethernet connection, and your PC's TCP/IP settings are good, then you should be able to access the Internet.

You may also try to ping your gateway (address should have been provided by your ISP). If everything looks OK on your modem and LAN and you are not able to ping your gateway, then the problem may be with the ISP router. On Windows based systems, you can try `ping www` at a DOS prompt. Please contact your ISP to help resolve this problem.

- **Quick Start says that it cannot detect the X320R.**

Quick Start automatically tries to detect the X320R over the Ethernet LAN. If it is not able to detect the X320R, check that your X320R is powered on and all cables are properly connected.

- **I can not connect to the serial port in terminal mode.**

Check that you have your serial port terminal settings correct:

- Serial Connection Speed: 115200 bps
- Data Bits: 8
- Parity: None
- Stop Bits: 1
- Flow Control: None

- **While trying to access the X320R using the web interface, I have entered the correct IP address but nothing happens.**

First check that the X320R is correctly connected to the LAN.

Then verify that the X320R and the PC, from which you are running your web browser, are on the same subnet. For example, the X320R has a default IP address of 192.168.1.1 and a subnet mask of 255.255.255.0. Your PC must have an address in the 192.168.1.X range, where X is a number between 2 and 254 (0, 1, and 255 are typically reserved addresses).

- **I added a new hub to one of the Ethernet ports on the X320R. The link light does not come on.**

To connect the X320R, which has an integrated hub, to another hub you have to do one of the following:

- Use a cross-over cable between the two hubs.
- Use a straight-thru cable, where one hub has an **uplink** switch enabled. Some hubs may instead have a special port (usually port 1) reserved for uplink.

- **I added a IP filter rule, but it is not working.**

Rules are executed in first-come-first-served fashion. For example, if Rule #1 blocks traffic to PC#2, and Rule#2 passes traffic to PC#2, then Rule #1 will have priority and traffic to PC#2 will be blocked.

- **My Service Provider does not understand what “Quat Swap” or “Inverted Bits” mean. What do those terms mean?**

Quat Swap refers to the order of bits in a 2B1Q.

Inverted Bits refers to the polarity of the bits.

The following table lists the typical required settings for various DSLAMs. You may have to contact your service provider to determine what DSLAM is used for

your service. You may use the table to determine the settings required for your router.

Vendor	Quat Swap	Inverted Bit
Copper Mountain	Off	Off
Interspeed	On	Off
Lucent - Max 20	On	On
Lucent - TNT	On	On

- **How do I contact technical support?**

If you are having trouble connecting to your DSL service, you must contact your ISP. If you are having physical trouble with your X320R router, please contact Xpeed Technical Support at 408-383-3810 or support@xpeed.com.

You may also browse the Xpeed support web-site: www.xpeed.com/support.

Appendix B

Frequently Asked Questions

- **Q: What operating systems does the Xpeed 320 support?**

The Xpeed 320 is OS independent. However, the Xpeed QuickStart software only works with Windows 95 updated with Winsock 2, Windows 98, Windows 98 - Second Edition, Windows NT, and Windows 2000.

- **Q: How do I get Winsock 2 for my Windows 95?**

If you're still using Windows 95, you'll need to install the Winsock 2 upgrade from Microsoft. Go to <http://www.microsoft.com/downloads/search.asp> and search for the Windows 95 Winsock 2 updates. After downloading Winsock 2 onto your Windows 95 PC, it should be ready to support the Xpeed QuickStart.

- **Q: I canceled the software installation before it was complete. What do I do?**

Just re-install the software. If you have problems, uninstall the software and then re-install it. To un-install the software, go to the **Windows Start**⇒**Settings**⇒**Control Panel**⇒**Add / Remove Programs**. Select the Xpeed software, remove it, then re-run the software installation.

- **Q: I am not able to connect at the maximum 2.3 Mbps. What's wrong?**

The actual maximum speed you are able to receive is determined by several conditions including your distance from the central office, and the quality of your line. You may contact your ISP to determine what your maximum may be and, if possible, upgrade your service to a higher class.

- **Q: The Internet connection is slower than usual. What's wrong?**

The X320 is able to handle data at very high speeds and it's unlikely to be the cause. If slow performance is seen only part time then, it may be caused by a busy LAN (someone is transferring big files between PC's or from a remote site) or perhaps the web site you're trying to reach is slow. If the connection is slow all the time you may want to contact your service provider and subscribe to a faster connection.

- **Q: When downloading and uploading data to the Internet at the same time, I am unable to get full speed transfers. How can I speed up my connection?**

This may be caused by excessive LAN or WAN bound traffic. It may also be caused by congestion on your service provider's network. Contact your DSL service provider for help.

- **Q: I have a number of PC's connected together on a local area network, and I would like all of them to have access to the internet via my one SDSL connection. How can I set this up?**

You can use a feature called Network Address Translation (NAT). An example of how to set this up is in the Applications section.

- **Q: What is QuickStart?**

Quick Start is a management utility. It provides a quick and easy way to make configuration changes in the router such as TCP/IP Address,

- **Q: What do I do if I lost my password?**

You will have to contact customer support to reset the X320R back to the basic configuration.

- **Q: My modem is currently configured to operate at _____ speed. Is there a setting that I can change to make it faster?**

No. The speed is predetermined. Changing the speed setting on your modem will not make it operate at a faster speed. Instead, your connection will be disabled since the DSLAM will expect a specific configuration from your modem.

- **Q: I lost my SDSL cable. Where can I order a new one?**

The SDSL line uses the center pair of conductors. If you loose the SDSL cable, you can use a standard telephone cable instead. However, the connector on the telephone cable may be smaller, so be sure that the connectors are seated properly.

- **Q: What kind of Ethernet cable can I use?**

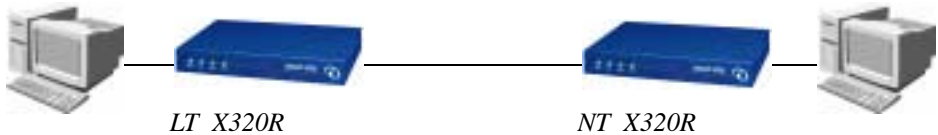
You may use any Category 5 Ethernet cable. These are commonly available through most computer retailers.

- **Q: How can I setup two X320's to operate in a back-to-back mode?**

Typically, your X320R will connect to a DSLAM at the central office. However, it is possible to connect two X320R units using a twisted pair line (up to 18 Kft). One unit may be left in Network Termination mode. The other unit must be configured to Line Termination mode.

WAN IP Addr = X.X.X.X
Mask = Z.Z.Z.Z
Gateway = Y.Y.Y.Y

WAN IP Addr = Y.Y.Y.Y
Mask = Z.Z.Z.Z
Gateway = X.X.X.X



- **Q: In the sample application, it allows up to 253 users. How do I add more?**

The sample application assumes that the typical small office or home office network will not exceed 253 PCs or nodes. However, if necessary, you may increase the size of your LAN by increasing your subnet.

A subnet of 255 . 255 . 255 . 0 provides 256 addresses, minus network ID, broadcast and gateway addresses.

A subnet of 255 . 255 . 252 . 0 (252 decimal = 11111100 binary) provides 1024 addresses, minus network ID, broadcast and gateway addresses.

- **Q: Where can I go for more information on DSL?**

A good introductory book is *DSL for Dummies*, by David Angell, published by IDG Books.

Appendix C

Default Settings

This section describes the default settings for the X320R. You may refer to this section as necessary for reference.

SERIAL PORT CONFIGURATION (CONSOLE)

- Serial Connection Speed: 115200 bps
- Data Bits: 8
- Parity: None
- Stop Bits: 1
- Flow Control: None
- Max Rows: 17

COMMUNITY

- None

DEBUG LEVEL

- None (0)

DEVICE

- Router

DHCP

- Range: 192.168.1.200 to 192.168.1.249
- Number of leases: 50 clients max
- Default Gateway: 192.168.1.1
- Default Lease Time: 10800
- Max Lease Time: 31536000
- Next Server: None (NULL)
- DHCP Client: Disable
- DHCP Server: Enable

DSLCONFIG

- PortID: W0
- QuatSwapped: No
- InvertedBitStream: No
- LinkSpeed: Auto Sensed

FILTER DEFAULTS:

- Block file sharing in & out, TCP/UDP port 137-139
- Block in & out UNIX NFS 2049
- Block UNIX RPC in & out port 111
- Block in TCP 109, 110, 143 (pop2, pop3, imac)

- Block short fragment (0 length packet)

FRCONFIG

- PortID: W0
- Termination: NT
- SwitchType: ANSI
- Lmi: Off

LAN INTERFACE

- DHCP Server: On
- Enabled: Yes
- Interface ID: L0
- IP Address: 192.168.1.1
- Subnet: 255.255.255.0

WAN INTERFACE

- DHCP Client : Off
- Enabled: Yes
- Framing Type: RFC1483MAC
- Interface ID: W0.0
- IP Address: 0.0.0.0
- Subnet: 0.0.0.0

NAT RULES

- None

PPPCONFIG

- PortID: W0
- Authentication: AUTO
- Chap Type: MD5
- PPP Enabled: No
- IP Header Compression: No
- User Id: None
- User Password: None

RIP

- LAN receive: On (receive both rip version 1 & 2 type packets)
- LAN send: No
- WAN receive: No
- WAN send: No

LOGIN USER ID & PASSWORD

- System Userid: system
- System Userid Password: system
- Guest Userid: guest
- Guest Userid Password: guest

SNMP MANAGEMENT

- Disabled

STATIC IP ROUTING

- Enabled

WEB MANAGEMENT

- Enabled

CLI MANAGEMENT

- Enabled

Appendix D

Technical Specifications

WAN INTERFACE

- Standard RJ45 jack
- Symmetrical Digital Subscriber Line (SDSL) interface
- Speeds up to 2.32 Mbps

LAN INTERFACE

- Integrated 4-port Ethernet 10BaseT hub

LED INDICATORS

- Power
- DSL Link
- LAN Activity
- WAN Activity

PROTOCOLS SUPPORTED

- RFC 1483 (MAC Encapsulated Frame Relay, LMI On or Off)
- RFC 1490 (MAC Encapsulated Frame Relay LMI On or Off)
- RFC 1490 Bridged Ethernet LMI On or Off
- MAC encapsulation
- PPP

DHCP

- DHCP Client
- DHCP Server (Maximum of 50 clients)

IP ROUTING

- RIP1 (receive only)
- RIP2 (send & receive)

POWER REQUIREMENTS

- AC voltage: 110 to 240 VAC
- Frequency: 50/60 Hz
- Power consumption: 3.5 W maximum

OPERATING ENVIRONMENT

- Temperature: 32°F - 158°F (0°C - 70°C)
- Humidity: 5% - 80%, non-condensing

PHYSICAL SPECIFICATIONS

- 7.8 W x 5.2 D x 1.3 H in.

- 19.8 W x 13.2 D x 2.7 H cm.
- Holes for wall mounting: 3 15/16" (10 cm) center to center

WARRANTY

One year limited warranty on parts and labor, factory repair or replacement.

Two-year and three-year extended warranties may be available. Contact reseller.

REGULATORY COMPLIANCE

FCC Part 15 Class A

NOTE: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference with the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

Appendix E

Glossary

10Base-T - A 10 MBPS Ethernet LAN that runs over twisted pair wiring. This network interface was originally designed to run over ordinary twisted pair (phone wiring) but is predominantly used with Category 3 or 5 cabling.

100Base-T - A 100 MBPS Ethernet LAN that runs over twisted pair wiring. It is the new Ethernet networking standard and is backward compatible with 10Base-T networks. Commonly referred to as Fast Ethernet.

2B1Q (Two Binary, One Quaternary) - A line coding technique used in SDSL and traditional telecommunications offerings, including ISDN.

Adapter card - Circuit board, usually installed in a personal computer, that provides the physical interface to a communications network. Also called a Network Interface Card (NIC).

ADSL (Asymmetric Digital Subscriber Line) - Asymmetric refers to the fact that the downstream bandwidth is high than the upstream bandwidth. This asymmetry is a good fit for video on demand and Internet access applications where large amounts of information is transmitted to the end-user, but little amounts of data is transmitted back up.

Always On - Refers to a feature of DSL where the connection to the Service Provider's network is always enabled in a way similar to a LAN. This is in contrast to traditional dial-up services, where users have to "dial-in" to setup a connection to the network.

Analog line - A communications line, such as ordinary phone line, that carries continuously varying signals.

Attenuation - Signal loss resulting from transversing the transmission medium.

Backbone - A major transmission path used for high-volume network-to-network connections. In DSL-to-Internet connections, a backbone network consolidates data traffic from the individual DSL lines into a backbone network for deliver to the ISP.

Bandwidth - The difference between the highest and lowest frequencies of a band that can be passed by a transmission medium without undo distortion. As a measure of carrying capacity, bandwidth indicates how many bits per second (bps) a link can carry.

bps (bits per second) - The rate of data transfer over a communication line.

Bridge - Bridging connects networks that use the same communications protocols. Bridging uses a MAC (media access control) address to locate and send information from one network to another.

Browser - See Web browser.

CAT-5 - Category 5 unshielded twisted pair wiring commonly used for 10Base-T and 100Base-T Ethernet networks.

CHAP (Challenge Handshake Authentication Protocol) - A security protocol that arranges an exchange of random numbers between computers. The machine receiving the number from the first computer performs calculations on that number using a previously agreed-upon string of characters as a secret encryption key.

CLEC (Competitive Local Exchange Carrier) - A telecommunications company that manages access to local loops.

Central Office (CO) - A building where the local switching equipment, including the DSLAM, is found.

CPE (Customer premises equipment) - Equipment residing at the customer/end-user's premises used to connect to the service provider's network.

Crosstalk - The interference caused by signals on adjacent circuits in a network, crosstalk is a hazard that limits distance and speed on digital networks.

Demarcation point - The point at the customer premises where the line from the telephone company meets the premises wiring. From the demarcation point, the end-user is responsible for the wiring.

DHCP (Dynamic Host Configuration Protocol) - A TCP/IP protocol that enables a network connected to the Internet to assign a temporary IP address to a host automatically when the host connects to the network. With dynamic addressing, a device can have a different IP address every time it connects to the network.

DHCP server - The server that assigns temporary IP addresses to a computer when it connects to the Internet.

DLCI (Data Link Connection Identifier) - The frame relay virtual circuit number used in internetworking to denote the port to which the destination LAN is attached.

DNS (Domain Name System) - An Internet service that translates domain names into IP addresses. For example, Xpeed.com will translate to 209.141.176.155.

Domain name - A name that identifies an IP address. For example, the domain name xpeed.com represents the IP address 209.141.176.155. Domain names are used in URLs to identify particular web pages.

Downstream - The direction of data flow on a data communications link, which occurs from the network down to the user. Typically used in conjunction with Upstream.

DSLAM (Digital Subscriber Line Access Multiplexer) - A CO platform for DSL modems that provides high-speed data transmission and optional POTS service simultaneously over traditional twisted-pair wiring.

Dynamic IP address - The address that the DHCP server assigns to the computer when the computer connects to the Internet.

Dynamic routing - The process of real-time routing changes in response to network changes. Dynamic routing software adjusts routes based on the routing update messages it receives, then distributes update messages about its new routes.

Encapsulation method - A method for transmitting multiple protocols within a particular network.

Ethernet - A type of network used to connect devices at speeds up to 10/100 Mbps. Based on Carrier Sense Multiple Access/Collision Detection (CSMA/CD),

Ethernet works by simply checking the wire before sending data. Sometimes two stations send at precisely the same time in which case a collision is detected and retransmission is attempted. Ethernet is a widely-implemented standard for LAN's. See also 10Base-T or 100Base-T.

Ethernet Hub - A networking device that allows many hosts to be connected together in a star configuration. Multiple hubs may be daisy-chained together increasing capacity and extending the range.

Firewall - A security device (hardware or software) that controls access from the Internet to a local network by using identification information associated with TCP/IP packets to make a decision about whether to allow or deny access. This decision is based on a set of defined rules that describe which packets or sessions are allowed.

Frame Relay - A high-speed connection-oriented packet switching WAN protocol using variable-length frames.

FTP (File Transfer Protocol) - The protocol used on the Internet for transferring files to and from remote computer systems.

Gateway - In networking, a combination of hardware and software that links two different types of networks. Gateways between e-mail systems, for example, allow users on different e-mail systems to exchange messages.

GUI (Graphical User Interface) - A program interface that takes advantage of the computer's graphics capabilities to make the program easier to use.

Host - A computer or any device connected to a TCP/IP network.

IEEE 803.2 - The protocol that defines an Ethernet network at the physical layer of network signaling and cabling.

Interface - In the context of the User's Guide, refers to the interface between the X320R and any network. For example, the L0 interface refers to the interface between the X320R and the LAN.

Interoperability - The ability of equipment from multiple vendors to communicate using standardized protocols.

IP (Internet Protocol) - A Layer 3 networking protocol used for Internet packet delivery. Keeps track of the Internet addresses for different nodes, routes outgoing messages, and recognizes incoming messages.

IP address - A 4-byte number uniquely defining each host on the Internet. Ranges of addresses are assigned by Internic, an organization formed for this purpose. Usually written in dotted-decimal notation with periods separating the bytes (for example, 134.177.244.57).

ISP (Internet Service Provider) - The telecommunications company providing subscriber access into the Internet.

Kft (Kilofeet) - A thousand feet.

Kbps (Kilo-bits per second) - A measurement of digital bandwidth where one Kbps equals one thousand bits per second.

LAN (Local Area Network) - A data network covering a small area, usually within the confines of a building or floors within a building. Ethernet is a common LAN protocol. See also WAN (Wide Area Network).

Last mile - Refers to the local loop and is the difference between a local telephone company office and the customer premises; a distance of about 3 miles or 4 kilometers.

Latency - The delay in time between the sending of a unit of data at one end of a connection until the receipt of that unit at the destination.

Layer - OSI reference model; each layer performs certain tasks to move the information from the sender to the receiver. Protocols within the layers define the tasks for the networks but not how the tasks are accomplished.

LMI - Local Management Interface

Local Loop - A generic term for the connection between the customer's premises and the telephone company's serving central office. The local loop is the pair of copper wires that connects the end user to the central office, which is the gateway to the telecommunications network.

LT (Line Termination) - Refers to the mode of an equipment that exists on the network side, terminating the end user's line. See also NT.

MAC address (Media Access Control address) - A Layer 2 hardware address that uniquely identifies each node of a network.

Mbps (Million bits per second) - A measurement of digital bandwidth where one Mbps equals one million bits per second.

NAT (Network Address Translation) - The translation of an Internet Protocol address (IP address) used within one network to a different IP address known within another network. One network is designated the inside network and the other is the outside. Typically, a company maps its local inside network addresses to one or more global outside IP addresses and unmaps the global IP addresses on incoming packets back into local IP addresses. This helps ensure security since each outgoing or incoming request must go through a translation process that also offers the opportunity to qualify or authenticate the request or match it to a previous request. NAT also conserves on the number of global IP addresses that a company needs and it lets the company use a single IP address in its communication with the world.

Network Protocol - The network protocol defines the rules and parameters for network communications.

NIC (Network Interface Card) - Circuit board, usually installed in a personal computer, that provides the physical interface to a communications network. Also called an adapter card.

NT (Network Termination) - Refers to the mode of an equipment that exists on the user's line, terminating the connection from the network. See also LT

Packet - A piece of information formatted for transmission over a network from one device to another. Data is broken up into packets for sending over a network, and each packet has a header containing source and destination addresses, an identification number, and error-checking code.

PAP (Password Authentication Protocol) - A security protocol that establishes a two-way handshake to verify the identity of the two computers.

PPP (Point-to-Point Protocol) - A method of connecting a computer to the Internet.

Protocol - A set of rules or standards that regulate data exchange between computers, including the rules for data transmission and the formatting of messages.

PVC (Permanent Virtual Circuit) - A term found in frame relay networking in which a virtual connection between two fixed end-points is established through the network.

RFC (Request for Comment) - A term for an IETF specification.

RIP (Routing Information Protocol) - A distance vector routing protocol popular for routing IP.

RJ-11 - Four-conductor modular jack used with four-wire cabling. This is the most common type of phone jack in the world and it is used commonly on phones, modems, and fax machines.

RJ-45 - Eight-pin connector used to attach data transmission devices to standard telephone wiring. Commonly used in 10Base-T connections.

Router - A device that connects LAN's by dynamically routing data according to network Layer 3 addressing on incoming and outgoing packets. Packet information is read and the packets are then forwarded to the appropriate end station.

RS-232 - An industry standard for serial communications connections.

SDSL (Symmetric Digital Subscriber Line) - SDSL technology allows data to travel at high speeds, both from client to server and server to client. Unlike ADSL, data travels at the same rate from either end of the connection.

SOHO - Small Office/Home Office.

Spoofing - A way to make a data transmission appear that it's coming from an authorized user. For example, in IP spoofing, the data transmission uses an IP address, which appears to come from an authorized user, to gain access to a computer or network. You can also use spoofing to help manage network traffic.

Static IP addressing - An assigned IP address used to connect to a TCP/IP network. The same IP number is used every time the connection to the network is made.

Subnet - A network that is a part of another network. Dividing a single logical network into smaller physical networks simplifies routing. The subnet shares a network address with the other parts of the network.

Subnet Mask - A 32-bit number used to separate the network and host sections of an IP address. A subnet mask subdivides an IP network into smaller pieces. An example of a subnet mask address might be 255.255.255.248 for an 8 IP address network.

TCP/IP (Transmission Control Protocol/Internet Protocol) - The protocol suite in the worldwide Internet, TCP is Layer 4, the transport layer. IP is Layer 3, the network layer.

TFTP Server (Trivial File Transfer Protocol) - A simplified version of FTP (File Transfer Protocol). Used to import and export configuration information to and from the TFTP server.

Upstream - The direction of information flow on a connection where data travels up from the user to the service provider.

VPN (Virtual Private Network) - A network that is constructed by using public wires to connect nodes. For example, a number of systems enable creation of networks using the Internet as the medium for transporting data. These systems use encryption and other security mechanisms to ensure that only authorized users can access the network and that the data cannot be intercepted.

WAN (Wide Area Network) - Network connection over public medium, such as telephone lines. Usually used to connect LANs together over a long distance.

Web browser - An application that allows users to view HTML documents from the World Wide Web on their computers.

WinSock - A program that conforms to a set of standards called the Windows Socket API (Application Programming Interface). A WinSock program controls the link between Microsoft Windows software and a TCP/IP program.

Index

A

ADSL 9
authentication 36

B

back-to-back mode 36, 87

C

cable 17, 87
chassis 11, 94
Command Line Interface 13, 45, 51
configuration information 16

D

DHCP 42, 76, 80, 90
DHCP Client 24, 35
DHCP Configuration 42
DHCP Server 34, 42
DSL Configuration 26, 37

E

Ethernet port 12

F

firmware 28, 44
Frame Relay Configuration 35

G

Glossary 97
group rule 38
guest 49

H

hub 17, 76, 83
HyperTerminal 46, 77

I

installation 19
Interface Configuration 34
Inverted Bit 26
Inverted Bits 60, 83
IP address 70
IP filter 38
IP-Filter Configuration 38
ISP 16

L

LAN Configuration 23, 34
LED 11, 81, 93
LMI 36
login 47, 77

N

NAT 37, 54, 72, 79, 86
NAT Map Configuration 40
NAT Redirect Configuration 41
netmask 71

P

password 43, 62, 90
ping 63, 82
port range 40
power supply 13, 94
PPP Configuration 16, 25, 36
Product Information 22, 33
protocols 89, 94

Q

Quat Swap 26, 60, 83
Quick Start 13, 21, 82, 86

R

Reboot 44, 63
requirements 17, 21
RIP 69
RIP2 Configuration 27, 37
Route Table Configuration 43, 54
router 69
rule 38

S

SDSL 9, 15
serial interface 12, 45, 77, 82
serial number 33
speed 13, 26, 37, 86
subnet 71
system 49

T

TELNET 13, 48

U

uplink 17, 83

V

version 23, 33

W

WAN Configuration 24, 35

web browser 13, 31, 32

web interface 31, 83

Winsock 21, 85

CLI Command Index

A

- add 51
- add arpentry 52
- add dhcpsubnet 52
- add dslconfig 53
- add frconfig 54
- add interface 54
- add nat 55
- add pppconfig 55
- add route 56
- alias 57

D

- delete 57
- delete arpentry 57
- delete interface 57
- delete route 58
- disable 58
- disable debug 58
- disable filter 58

E

- enable 59
- enable debug 59
- enable filter 59
- exit 60

H

- help 60

L

- logout 60

M

- modify 61
- modify console 61
- modify dslconfig 61
- modify frconfig 61
- modify interface 62
- modify tcpip 62

P

- ping 63

Q

quit 64

R

reboot 64

restore 64

S

save 65

show 65

show all 65

show arp 65

show console 66

show debug level 67

show dslconfig 66

show frconfig 66

show interface 66

show route 67

show sysconfig 67

show tcpip 67

T

tftp 67

traceroute 68

U

unalias 68

Software License Agreement

Use of the enclosed software program, "Software", is subject to the software license terms set forth below. Using the Software indicates your acceptance of these license terms. If you do not accept these license terms, you must return the unused product, all manuals and documentation, and proof of purchase, to the place of purchase for a full refund.

Xpeed, Inc. and its suppliers grant you a nonexclusive license to use one copy of the Software. The Software is in use if it is loaded on the computer's permanent or temporary memory. You may make two copies of the Software only for backup and archival purposes. No other rights are granted.

You may not disassemble, de-compile, reverse-engineer, or modify the Software in any way without the prior written consent of Xpeed, Inc.

The Software is owned and copyrighted by Xpeed, Inc. and its licensors. Your license confers no title to, or ownership in, the Software and is not a sale of any rights to the Software.

Your license will automatically terminate upon any transfer of the Software. Upon transfer, you must deliver the Software, including any copies and related documentation, to the transferee. The transferee must accept these license terms as a condition to the transfer.

Xpeed, Inc. may terminate your license upon notice for failure to comply with any of these license terms. Upon termination, you must immediately destroy all copies and/or versions of the Software.